LAW OFFICES
SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037-3213
TELEPHONE (202) 293-7060
FACSIMILE (202) 293-7860
www.sughrue.com

#7

April 20, 2001

BOX PATENT APPLICATION
Commissioner for Patents
Washington, D.C. 20231

Re: Application of Tomoya SAEKI
PERSONAL AUTHENTICATION SYSTEM,
AND PERSONAL AUTHENTICATION
METHOD AND PROGRAM USED THEREFOR
Our Ref. Q64153

Dear Sir:

Attached hereto is the application identified above including 51 sheets of the specification, including the claims and abstract, 15 sheets of formal drawings, executed Assignment and PTO 1595 form, and executed Declaration and Power of Attorney.

The Government filing fee is calculated as follows:

Total claims	42	-	20	=	22	x	$18.00	=	$396.00
Independent claims	3	-	3	=		x	$80.00	=	$.00
Base Fee									$710.00
TOTAL FILING FEE									**$1106.00**
Recordation of Assignment									$40.00
TOTAL FEE									**$1146.00**

Checks for the statutory filing fee of $1106.00 and Assignment recordation fee of $40.00 are attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 and any petitions for extension of time under 37 C.F.R. § 1.136 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

Priority is claimed from April 26, 2000 based on Japanese Application No. 125062/2000. The priority document is enclosed herewith.

Respectfully submitted,
SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
Attorneys for Applicant

By: _____
J. Frank Osha
Registration No. 24,625

T. Saeki
4/20/01
Q64153
1 of 1

JC997 U.S. PTO
09/838319
04/20/01

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　４月２６日

出願番号
Application Number: 特願２０００－１２５０６２

出願人
Applicant (s): 新潟日本電気株式会社

２００１年　２月　９日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３００６９２５

【書類名】　特許願

【整理番号】　03130808

【提出日】　平成12年 4月26日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/00

【発明者】

【住所又は居所】　新潟県柏崎市大字安田７５４６番地　新潟日本電気株式会社内

【氏名】　佐伯　智也

【特許出願人】

【識別番号】　000190541

【氏名又は名称】　新潟日本電気株式会社

【代理人】

【識別番号】　100088812

【弁理士】

【氏名又は名称】　▲柳▼川　信

【手数料の表示】

【予納台帳番号】　030982

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　個人認証システム及びそれに用いる個人認証方法

【特許請求の範囲】

【請求項１】　顧客が本人であることを証明するための個人認証を行う認証サーバと前記個人認証を行うための認証情報を入力する認証端末とを通信回線を介して相互に接続する個人認証システムであって、

予め登録される前記個人認証を行うための個人認証データと費用処理するための決済口座の情報と各種サービスを受けるために必要なデータとを少なくとも蓄積するデータベースを有し、

前記認証端末から前記通信回線を介して入力される前記認証情報を前記データベースに蓄積された前記個人認証データと照会して本人確認を行う機能と、前記本人確認で認証された時に前記認証端末からの要求に基づいて前記データベースに登録された前記決済口座の情報を基に費用処理する機能と、前記本人確認で認証された時に前記認証端末からの要求に基づいて前記データベースに予め登録された個人データの提供と登録と管理とを行いかつそれらの照会履歴と個人データ利用履歴と費用処理履歴とを定期的に通知する機能とを前記認証サーバに有することを特徴とする個人認証システム。

【請求項２】　前記本人確認で認証された時に前記認証端末からの要求に基づいて前記各種サービスの許可を通知する機能を前記認証サーバに含むことを特徴とする請求項１記載の個人認証システム。

【請求項３】　前記個人認証データは、顧客の指紋と顧客の声紋と顧客の虹彩パターンと予め設定されたパスワードとのうちの少なくとも一つであることを特徴とする請求項１または請求項２記載の個人認証システム。

【請求項４】　前記照会履歴と前記個人データ利用履歴と前記費用処理履歴とを通知する機能は、それらの情報を電子メールにて通知するよう構成したことを特徴とする請求項１から請求項３のいずれか記載の個人認証システム。

【請求項５】　前記照会履歴と前記個人データ利用履歴と前記費用処理履歴とを通知する機能は、それらの情報をホームページに掲示するよう構成したこと

を特徴とする請求項１から請求項４のいずれか記載の個人認証システム。

【請求項６】　前記ホームページは、予め登録された顧客のみにその閲覧を許可するようにしたことを特徴とする請求項５記載の個人認証システム。

【請求項７】　前記認証端末は店舗に設置され、商品及びサービスの少なくとも一方を提供する際に前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に提供した商品及びサービスの対価を前記決済口座から決済することを前記認証サーバに要求するよう構成したことを特徴とする請求項１から請求項６のいずれか記載の個人認証システム。

【請求項８】　前記認証端末は公共交通機関の改札に設置され、前記公共交通機関の利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に前記公共交通機関の利用区間に相当する代金を前記決済口座から決済することを前記認証サーバに要求するよう構成したことを特徴とする請求項１から請求項６のいずれか記載の個人認証システム。

【請求項９】　前記認証端末の機能は公衆電話に付加され、前記公衆電話の利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に前記公衆電話の通話料金を前記決済口座から決済することを前記認証サーバに要求するよう構成したことを特徴とする請求項１から請求項６のいずれか記載の個人認証システム。

【請求項１０】　前記認証端末は病院窓口に設置され、前記病院の利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に認証された顧客のカルテ及び各種検査データの個人情報を引出すとともに前記病院の医療費用を前記決済口座から決済することを前記認証サーバに要求するよう構成したことを特徴とする請求項１から請求項６のいずれか記載の個人認証システム。

【請求項１１】　前記認証端末は官公庁の各種手続き窓口に設置され、前記各種手続きの利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に前記各種手続きの申請を受理するとともにその手数料金を前記決済口座から決済することを前記認証サーバに要求するよう構成したことを特徴とする請求項１から請求項６のいずれか記載の個人認証システム。

【請求項１２】　前記認証端末は各種サービス提供施設に設置され、前記各種サービス提供施設の利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に前記各種サービス提供施設の利用を許可するとともにそのサービス料金を前記決済口座から決済することを前記認証サーバに要求するよう構成したことを特徴とする請求項１から請求項６のいずれか記載の個人認証システム。

【請求項１３】　前記認証端末は入退場が制限されている施設の入退場口に設置され、前記施設の利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に入退場の許可及び管理を行うよう構成したことを特徴とする請求項１から請求項６のいずれか記載の個人認証システム。

【請求項１４】　前記認証端末は証明書類の発行及びそれに関する登録を行う手続窓口に設置され、前記証明書類の発行及びそれに関する登録を利用する際に前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に前記証明書類の発行及びそれに関する登録を許可するとともにその手数料金を前記決済口座から決済することを前記認証サーバに要求するよう構成したことを特徴とする請求項１から請求項６のいずれか記載の個人認証システム。

【請求項１５】　顧客が本人であることを証明するための個人認証を行う認証サーバと前記個人認証を行うための認証情報を入力する認証端末とを通信回線を介して相互に接続する個人認証システムの個人認証方法であって、

予め登録される前記個人認証を行うための個人認証データと費用処理するための決済口座の情報と各種サービスを受けるために必要なデータとを少なくとも蓄積するデータベースを有し、

前記認証端末から前記通信回線を介して入力される前記認証情報を前記データベースに蓄積された前記個人認証データと照会して本人確認を行うステップと、前記本人確認で認証された時に前記認証端末からの要求に基づいて前記データベースに登録された前記決済口座の情報を基に費用処理するステップと、前記本人確認で認証された時に前記認証端末からの要求に基づいて前記データベースに予め登録された個人データの提供と登録と管理とを行いかつそれらの照会履歴と個人データ利用履歴と費用処理履歴とを定期的に通知するステップとを前記認証サ

ーバに有することを特徴とする個人認証方法。

【請求項１６】　前記本人確認で認証された時に前記認証端末からの要求に基づいて前記各種サービスの許可を通知するステップを前記認証サーバに含むことを特徴とする請求項１５記載の個人認証方法。

【請求項１７】　前記個人認証データは、顧客の指紋と顧客の声紋と顧客の虹彩パターンと予め設定されたパスワードとのうちの少なくとも一つであることを特徴とする請求項１５または請求項１６記載の個人認証方法。

【請求項１８】　前記照会履歴と前記個人データ利用履歴と前記費用処理履歴とを通知するステップは、それらの情報を電子メールにて通知するようにしたことを特徴とする請求項１５から請求項１７のいずれか記載の個人認証方法。

【請求項１９】　前記照会履歴と前記個人データ利用履歴と前記費用処理履歴とを通知するステップは、それらの情報をホームページに掲示するようにしたことを特徴とする請求項１５から請求項１８のいずれか記載の個人認証方法。

【請求項２０】　前記ホームページは、予め登録された顧客のみにその閲覧を許可するようにしたことを特徴とする請求項１９記載の個人認証方法。

【請求項２１】　前記認証端末は店舗に設置され、商品及びサービスの少なくとも一方を提供する際に前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に提供した商品及びサービスの対価を前記決済口座から決済することを前記認証サーバに要求するようにしたことを特徴とする請求項１５から請求項２０のいずれか記載の個人認証方法。

【請求項２２】　前記認証端末は公共交通機関の改札に設置され、前記公共交通機関の利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に前記公共交通機関の利用区間に相当する代金を前記決済口座から決済することを前記認証サーバに要求するようにしたことを特徴とする請求項１５から請求項２０のいずれか記載の個人認証方法。

【請求項２３】　前記認証端末の機能は公衆電話に付加され、前記公衆電話の利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に前記公衆電話の通話料金を前記決済口座から決済することを前記認証サーバに要求するようにしたことを特徴とする請求項１５から請求項２０

のいずれか記載の個人認証方法。

【請求項２４】　前記認証端末は病院窓口に設置され、前記病院の利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に認証された顧客のカルテ及び各種検査データの個人情報を引出すとともに前記病院の医療費用を前記決済口座から決済することを前記認証サーバに要求するようにしたことを特徴とする請求項１５から請求項２０のいずれか記載の個人認証方法。

【請求項２５】　前記認証端末は官公庁の各種手続き窓口に設置され、前記各種手続きの利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に前記各種手続きの申請を受理するとともにその手数料金を前記決済口座から決済することを前記認証サーバに要求するようにしたことを特徴とする請求項１５から請求項２０のいずれか記載の個人認証方法。

【請求項２６】　前記認証端末は各種サービス提供施設に設置され、前記各種サービス提供施設の利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に前記各種サービス提供施設の利用を許可するとともにそのサービス料金を前記決済口座から決済することを前記認証サーバに要求するようにしたことを特徴とする請求項１５から請求項２０のいずれか記載の個人認証方法。

【請求項２７】　前記認証端末は入退場が制限されている施設の入退場口に設置され、前記施設の利用に際して前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に入退場の許可及び管理を行うようにしたことを特徴とする請求項１５から請求項２０のいずれか記載の個人認証方法。

【請求項２８】　前記認証端末は証明書類の発行及びそれに関する登録を行う手続窓口に設置され、前記証明書類の発行及びそれに関する登録を利用する際に前記本人確認を行うよう前記認証サーバに要求し、前記本人確認で認証された時に前記証明書類の発行及びそれに関する登録を許可するとともにその手数料金を前記決済口座から決済することを前記認証サーバに要求するようにしたことを特徴とする請求項１５から請求項２０のいずれか記載の個人認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は個人認証システム及び各種サービスに用いられる個人認証方法に関し、特にクレジットサービスや医療サービス等の各種サービスにおける個人認証方法に関する。

【０００２】

【従来の技術】

従来、クレジットサービスにおいては、商品の購入やサービスの提供を受ける際にクレジット会社を利用する場合、予めクレジット会社から発行されたクレジットカードを提示し、商品あるいはサービスの対価が記載された書類に署名することで、後刻、予めクレジット会社に登録した個人決済口座にて当該対価の決済を行っている。

【０００３】

また、インタネット等におけるオンラインでの商品の購入やサービスの提供を受ける場合には、クレジット会社から発行されたクレジット番号、発行年月、簡単な数字の組合せからなるパスワードによって個人認証を行うことで、予めクレジット会社に登録した個人決済口座にて当該対価の決済を行っている。

【０００４】

さらに、電話やデータ通信等で一般の公衆回線サービスを利用する際の代金決済にクレジット会社を利用する場合にも、クレジット会社から発行されたクレジット番号、発行年月、簡単な数字の組合せからなるパスワードによって個人認証を行うことで、予めクレジット会社に登録した個人決済口座にて当該対価の決済を行っている。この場合、電話会社から発行されているプリペイドカードを利用することで、対価の決済を行うことも可能である。

【０００５】

さらにまた、病院にて受診する際には、窓口にて病院の発行する受診カードを提示してカルテや検査データ等を受取り、医師の診察や治療を受けた後、再度、窓口にてカルテの返却並びに医療費の支払いを行っている。

【０００６】

一方、官公庁において旅券や運転免許証その他各種の資格、免許の申請を行う際には、住民票の写しや戸籍抄本、あるいは戸籍謄本等の書類を取り寄せ、また申請窓口においても本人を証明する身分証明書を提示して事務手続きを行っている。

【０００７】

また、図書館で図書の貸し出しを受ける際には、予め身分証明書を提示し、利用カードの作成や発行を受け、この利用カードを利用する毎に毎回提示するようになっている。

【０００８】

さらに、スポーツジム等の会員制での設備提供、あるいはサービスの提供を受ける場合には、予め登録事務手続きを行い、一般的には発行される会員証を提示することで、これら設備の提供やサービスの提供を受けている。この会員証も毎回提示するようになっている。

【０００９】

個人や法人の敷地、建物等の入退場が制限されている施設の入退場管理は、予め発行された入場許可証や身分証明書等を提示したり、予め登録されたパスワードを照合することで行われている。

【００１０】

【発明が解決しようとする課題】

しかしながら、上述した従来の個人認証システムでは、商品の購入やサービスの提供を受ける際にクレジットカードを提示することで、クレジット会社のサービスを利用する場合、クレジットカードの所持携行を忘れたり、クレジットカードを紛失すると、これらのサービスの提供を受けることができず、また第３者に悪用される恐れもある。また、クレジットカードを偽造された場合には、これらのサービスを違法に利用される恐れもある。

【００１１】

また、インタネット等のオンラインで、商品の購入やサービスの提供を受ける際にクレジット会社のサービスを利用する場合には、クレジットカード番号、発行年月、パスワードの情報が必要であり、これらの情報が不明の場合には本人で

あってもこれら商品やサービスの提供を受けることができない。この場合、これらの情報は容易に入手、利用することができるため、第３者に悪用される恐れもある。

【００１２】

さらに、一般の公衆回線サービスを利用する際の代金決済手段としては、現金の他、プリペイドカードやクレジット会社のサービスを利用することができるが、いずれも上記のようなカードや情報が必要であり、現金やカードを所持携行していなかったり、あるいはクレジットサービスに必要な情報が不明であったりすると、正規に利用可能な本人であっても利用することができないばかりか、カード偽造による違法利用の恐れもある。

【００１３】

さらにまた、病院にて受診する際に、病院発行の受診カードを提示することで本人特定を行っているために、紛失した受診カードや偽造した受診カードを悪用されることで、病歴等の個人情報が流出する恐れがある。この場合、医療費の支払いにクレジット会社のサービスを利用する場合には、受診カードとは別にクレジットカードの所持携行が必要であり、これを忘れたり、クレジットカードを紛失すると、これらサービスの提供を受けることができない。

【００１４】

官公庁における各種の資格や免許の申請を行う際には、住民票の写しや戸籍抄本あるいは戸籍謄本等の書類を事前に準備し、また申請窓口においても本人を証明する身分証明書の提示が必要であり、事務手続きが煩雑である。

【００１５】

また、図書館で図書の貸し出しを受ける際には、予め発行された利用カードを提示する必要があり、所持携行を忘れた場合には貸し出しを受けることができず、また紛失した場合には再発行の手続きが必要となり、利用カードの管理が煩雑である。

【００１６】

さらに、会員制で設備やサービスの提供を受ける場合には、予め発行された会員証を提示する必要があり、会員証の所持携行を忘れた場合には設備やサービス

の提供を受けることができず、また紛失した場合にはこれを悪用される恐れもある。

【００１７】

さらにまた、個人や法人の敷地、建物等の入退場が制限されている施設の入退場には、予め発行された入場許可証や身分証明書等を提示したり、予め登録されたパスワードを照合する必要があり、これらを忘れた場合には入退場に支障をきすばかりか、これらを紛失あるいは流出することによって第３者が違法に入退場する恐れもある。

【００１８】

そこで、本発明の目的は上記の問題点を解消し、カード類を所持携行することなくサービスの提供を受けることができ、カード類の第３者による盗用や偽造等の悪用を防止することができるとともに、個人情報の流出を防止することができる個人認証システム及び各種サービスに用いられる個人認証方法を提供することにある。

【００１９】

【課題を解決するための手段】

本発明による個人認証システムは、顧客が本人であることを証明するための個人認証を行う認証サーバと前記個人認証を行うための認証情報を入力する認証端末とを通信回線を介して相互に接続する個人認証システムであって、

予め登録される前記個人認証を行うための個人認証データと費用処理するための決済口座の情報と各種サービスを受けるために必要なデータとを少なくとも蓄積するデータベースを備え、

前記認証端末から前記通信回線を介して入力される前記認証情報を前記データベースに蓄積された前記個人認証データと照会して本人確認を行う機能と、前記本人確認で認証された時に前記認証端末からの要求に基づいて前記データベースに登録された前記決済口座の情報を基に費用処理する機能と、前記本人確認で認証された時に前記認証端末からの要求に基づいて前記データベースに予め登録された個人データの提供と登録と管理とを行いかつそれらの照会履歴と個人データ利用履歴と費用処理履歴とを定期的に通知する機能とを前記認証サーバに備えて

いる。

【００２０】

本発明による各種サービスに用いられる個人認証方法は、顧客が本人であることを証明するための個人認証を行う認証サーバと前記個人認証を行うための認証情報を入力する認証端末とを通信回線を介して相互に接続する個人認証システムの個人認証方法であって、

予め登録される前記個人認証を行うための個人認証データと費用処理するための決済口座の情報と各種サービスを受けるために必要なデータとを少なくとも蓄積するデータベースを備え、

前記認証端末から前記通信回線を介して入力される前記認証情報を前記データベースに蓄積された前記個人認証データと照会して本人確認を行うステップと、前記本人確認で認証された時に前記認証端末からの要求に基づいて前記データベースに登録された前記決済口座の情報を基に費用処理するステップと、前記本人確認で認証された時に前記認証端末からの要求に基づいて前記データベースに予め登録された個人データの提供と登録と管理とを行いかつそれらの照会履歴と個人データ利用履歴と費用処理履歴とを定期的に通知するステップとを前記認証サーバに備えている。

【００２１】

すなわち、本発明の個人認証システムは、通信回線と、この通信回線に相互に接続される認証サーバと、顧客端末と、認証端末とを備えたオンラインクレジットサービスであることを特徴とする。

【００２２】

認証サーバは顧客が本人であることを証明する個人認証データと、費用処理する決済口座と、その他各種サービスを受けるに必要なデータとを登録及び管理する。また、認証サーバは認証端末からの要求に基づいて個人認証データを照会し、本人と認証された個人に対して予め登録された決済口座から認証端末の要求に基づいて費用を処理し、必要であれば認証端末からの要求に基づいて認証された個人に対して予め登録された個人データを提供、登録、管理し、これら照会履歴、個人データ利用履歴、並びに費用処理履歴を顧客端末に定期的に通知する機能

を有している。

【００２３】

認証サーバにおける個人認証には、顧客の指紋、顧客の声紋、顧客の虹彩パターンをそれぞれ用いることが可能であり、顧客が入力するパスワードを使用して個人認証を行うことも可能である。

【００２４】

認証された個人に対する個人データ、照会履歴、個人データ利用履歴、並びに費用処理履歴を顧客端末に通知する方法としては、電子メールによる通知やホームページを利用することが可能である。

【００２５】

上記の認証端末やその機能の設置場所としては、店舗、公共交通機関の改札、公衆電話、病院窓口、官公庁の各種手続き窓口、図書館やスポーツジム等の各種サービス提供施設、個人や法人の敷地、建物等の入退場が制限されている施設の入退場口等がある。

【００２６】

これによって、本発明は個人認証サービスを提供するものであり、特にインタネット等のネットワークを介して顧客が本人であることを認証し、また必要であれば商品の購入やサービスの対価の決済、及び予め登録された個人データの利用サービスを実現可能とするものである。

【００２７】

【発明の実施の形態】

次に、本発明の実施例について図面を参照して説明する。図１は本発明の第１の実施例による個人認証システムの構成を示すブロック図である。図１において、本発明の第１の実施例による個人認証システムは認証サーバ１と、データベース２と、顧客端末３と、認証端末４とから構成され、認証サーバ１と顧客端末３と認証端末４とはインタネット等の通信回線１００によって相互に接続されている。

【００２８】

本発明の第１の実施例による個人認証システムを利用する場合、まず最初に、

顧客は顧客端末３あるいはインタネット等の通信回線１００経由で認証サーバ１に接続された端末（図示せず）による処理、あるいは郵送やファクシミリその他のオフライン手段等によって認証サーバ１に接続されたデータベース２に顧客が本人であることを証明する個人認証データ並びに顧客が購入した商品やサービスの対価支払いのための決済口座、その他認証サーバ１が提供する各種サービスに必要な個人データを登録しておく。

【００２９】

続いて、顧客は認証端末４を用いて顧客が本人であることを証明するデータを認証サーバ１に送付する。認証サーバ１は認証端末４から送付されてきたデータと予めデータベース２に登録してある個人認証データとを照合することによって本人であるかを確認し、その結果を認証端末４に送付する。

【００３０】

また、この認証後に、顧客が必要に応じて認証端末４を用いて、認証サーバ１のデータベース２に予め登録してある決済口座からの費用支払いを認証サーバ１に要求すると、認証サーバ１は送付された要求に基づいて処理を行う。

【００３１】

上記の費用支払い以外にも、顧客は必要に応じて認証端末４を用い、認証サーバのデータベース２に予め登録してある個人データの読出し、修正、新規登録等を認証サーバ１に要求し、認証サーバ１は送付された要求に基づいて処理を行う。認証サーバ１はこれらの個人認証照会や個人データへのアクセスの履歴を顧客に通知する。

【００３２】

図２及び図３は図１の認証サーバ１の処理動作を示すフローチャートである。これら図１～図３を参照して本発明の第１の実施例による個人認証システムの処理動作について説明する。

【００３３】

認証サーバ１は顧客端末３からの個人データの登録であれば（図２ステップＳ１）、顧客が本人であることを証明する個人認証データ、顧客が購入した商品やサービスの対価支払いのための決済口座、その他の認証サーバ１が提供する各種

サービスに必要な個人データをデータベース２に登録する（図２ステップＳ２）。また、認証サーバ１は認証端末４からの個人認証データの送付であれば（図２ステップＳ３）、送付されたデータと予めデータベース２に登録してある個人認証データとを照合し（図２ステップＳ４）、顧客が本人であるかどうかを確認する（図２ステップＳ５）。

【００３４】

認証サーバ１はこの個人認証において不一致を検出すると、本人でないことを認証端末４に送付し（図２ステップＳ６）、一致を検出すると、本人であることを認証端末４に送付する（図２ステップＳ７）。

【００３５】

認証サーバ１は本人であることを認証端末４に送付した後、つまり認証後に認証端末４から処理要求が送付されてくると（図２ステップＳ８）、認証端末４から送付された処理要求を実行する（図２ステップＳ９）。認証サーバ１は上記の処理動作をすべての処理が終了するまで繰返し実行する（図２ステップＳ１０）。

【００３６】

一方、認証サーバ１は認証端末４から要求される各種処理を実行する場合、まず顧客が認証されているかどうかを確認し（図３ステップＳ１１）、認証されていればその種別を判定する。

【００３７】

認証サーバ１は費用支払い要求の場合（図３ステップＳ１２）、データベース２に予め登録してある決済口座からの費用支払い処理を実行する（図３ステップＳ１３）。また、認証サーバ１は個人データの読出し要求の場合（図３ステップＳ１４）、データベース２に予め登録してある個人データを読出して通知処理を実行する（図３ステップＳ１５）。さらに、認証サーバ１は個人データの修正要求の場合（図３ステップＳ１６）、データベース２に予め登録してある個人データを読出して修正処理を実行し、データベース２の内容を更新する（図３ステップＳ１７）。

【００３８】

認証サーバ１は上述した各要求に対する処理を実行した後、データベース２内の個人認証照会や個人データへのアクセスの履歴を顧客に通知する（図３ステップＳ１８）。認証サーバ１は上記の処理動作をすべての処理が終了するまで繰返し実行する（図３ステップＳ１９）。

【００３９】

このように、認証サーバ１はインタネット等のネットワークを介して顧客が本人であることを認証し、また必要であれば商品の購入やサービスの対価の決済、及び予め登録された個人データの利用サービスを実現することができる。よって、カード類の所持携行を忘れたりあるいはカード類を紛失した場合でもサービスの提供を受けることができ、カード類の第３者による悪用を防止することができるとともに、個人情報の流出を防止することができる。

【００４０】

図４は本発明の第２の実施例による個人認証システムの構成を示すブロック図である。図４において、本発明の第２の実施例による個人認証システムは個人認証データ入力機構５を設けた以外は図１に示す本発明の第１の実施例による個人認証システムと同様の構成となっており、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の第１の実施例による個人認証システムと同様である。

【００４１】

個人認証データ入力機構５は指紋や声紋、及び虹彩パターン等の顧客個人に特有かつ個別なデータを個人認証データとして用いる場合に、その個人認証データを入力するためのものである。尚、顧客各々が入力するパスワードは認証端末４及び個人認証データ入力機構５のいずれからも入力可能となっている。

【００４２】

図５は本発明の第３の実施例による認証サーバの処理動作を示すフローチャートである。この図５を参照して本発明の第３の実施例による個人認証システムの処理動作について説明する。ここで、図５のステップＳ２８，Ｓ２９を除く他のステップは図３のステップＳ１１～Ｓ１７，Ｓ１９と同様の動作であり、その動作については説明を省略する。また、本発明の第３の実施例による個人認証シス

テムの構成は図１に示す本発明の第１の実施例による個人認証システムまたは図４に示す本発明の第２の実施例による個人認証システムの構成と同様であるので、その説明は省略する。

【００４３】

本発明の第３の実施例による個人認証システムでは、予め設定された指定日時（例えば、月に１回等）になると（図５ステップＳ２８）、顧客に対して定期的に、個人認証照会や個人データへのアクセスの履歴を電子メールによって通知している（図５ステップＳ３０）。また、予め設定された指定日時（例えば、月に１回等）にならなければ（図５ステップＳ２８）、その履歴を記録する（図５ステップＳ２９）。尚、個人認証照会や個人データへのアクセスの履歴の電子メールによる通知は処理（アクセス）の終了毎に行うことも可能である。

【００４４】

図６は本発明の第４の実施例による個人認証システムの構成を示すブロック図である。図６において、本発明の第４の実施例による個人認証システムはホームページを掲示する掲示用サーバ６と、ファイアウォール等の本人確認機構７とを設けた以外は図４に示す本発明の第２の実施例による個人認証システムと同様の構成となっており、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の第２の実施例による個人認証システムと同様である。

【００４５】

掲示用サーバ６は認証サーバ１に接続するように併設され、本人確認機構７を介してインタネット１００に接続されている。また、掲示用サーバ６は個人認証照会や個人データへのアクセスの履歴が記載されたホームページを掲示している。

【００４６】

ここで、本人確認機構７は本人以外参照できないよう暗号化やパスワード等の本人確認のセキュリティ等の対策をとって掲示用サーバ６に接続するようにしている。よって、顧客端末３は本人確認機構７で確認されると、インタネット１００を通して掲示用サーバ６のホームページの閲覧によって個人認証照会や個人データへのアクセスの履歴を読出すことができる。

【００４７】

図７は図６の認証サーバ１の処理動作を示すフローチャートである。この図７を参照して本発明の第３の実施例による個人認証システムの処理動作について説明する。ここで、図７のステップＳ４８を除く他のステップは図３のステップＳ１１～Ｓ１７，Ｓ１９と同様の動作であり、その動作については説明を省略する。

【００４８】

認証サーバ１は認証端末４からの要求に対する処理が終了すると、その処理結果、すなわち個人認証照会や個人データへのアクセスの履歴でホームページ内容を更新して掲示する（図７ステップＳ４８）。これによって、顧客に対応するホームページ上には常に最新のデータが掲示されることとなる。

【００４９】

図８は本発明の第５の実施例による認証サーバの処理動作を示すフローチャートである。この図８を参照して本発明の第５の実施例による認証サーバの処理動作について説明する。ここで、本発明の第５の実施例による個人認証システムのは図１に示す本発明の第１の実施例による個人認証システム、または図４に示す本発明の第２の実施例による個人認証システム、あるいは図６に示す本発明の第４の実施例による個人認証システムを店舗サービスに適用した例であり、その構成及び動作は本発明の第１～第４の実施例による個人認証システムと同様であるので、それらの説明については省略する。

【００５０】

本発明の第５の実施例による個人認証システムでは、認証端末４を店舗内に設置しており、顧客はこの店舗において商品やサービスの提供を受ける。顧客はその対価を支払う際に、指紋、声紋、虹彩パターン、パスワード等の顧客が予め認証サーバ１のデータベース２に登録してある個人認証データを、インタネット等の通信回線１００経由で認証サーバ１に接続された認証端末４を用いて照合し、同じく認証サーバ１に登録してある決済口座からの対価の支払いを要求する。認証サーバ１は認証端末４から送付されたデータによって顧客本人であることを照合した後、送付された要求に基づいて上記の支払い処理を行う。

【００５１】

すなわち、認証サーバ１は認証端末４からの個人認証データの送付であれば（図８ステップＳ５１）、送付されたデータと予め登録してある個人認証データとを照合し（図８ステップＳ５２）、顧客が本人であるかどうかを確認する（図８ステップＳ５３）。

【００５２】

認証サーバ１はこの個人認証において不一致を検出すると、本人でないことを認証端末４に送付し（図８ステップＳ５４）、一致を検出すると、本人であることを認証端末４に送付する（図８ステップＳ５５）。この一致を検出した時、認証サーバ１はデータベース２に予め登録してある決済口座からの対価の支払いの処理を実行する（図８ステップＳ５６）。

【００５３】

これによって、商品やサービスの提供を受ける際にクレジット会社のサービスを利用する場合に、従来、一般的であったクレジットカードが不要であるため、クレジットカードの所持携行を忘れたり、あるいはクレジットカードを紛失したためにサービスの提供を受けることができないということがない。この場合、紛失したクレジットカードが第３者に悪用される恐れがない。

【００５４】

また、インタネット等のオンラインで商品やサービスの提供を受ける際にクレジット会社のサービスを利用する場合、従来、一般的であったクレジットカードの番号、発行年月、パスワード等の入力が不要となるので、これらの情報が不明であるためにサービスの提供を受けることができないということがなくなる。また、これらの情報が不要となるため、これらの情報を第３者に悪用される恐れがない。

【００５５】

図９は本発明の第６の実施例による認証サーバの処理動作を示すフローチャートである。この図９を参照して本発明の第６の実施例による認証サーバの処理動作について説明する。ここで、本発明の第６の実施例による個人認証システムの構成及び動作は図１に示す本発明の第１の実施例による個人認証システム、また

は図４に示す本発明の第２の実施例による個人認証システム、あるいは図６に示す本発明の第４の実施例による個人認証システムを交通機関サービスに適用した例であり、その構成及び動作は本発明の第１～第４の実施例による個人認証システムと同様であるので、それらの説明については省略する。

【００５６】

本発明の第６の実施例による個人認証システムでは、認証端末４を公共交通機関の改札に設置している。顧客は改札を通過する際に、上記と同様の手順によって個人認証を行う。

【００５７】

認証端末４は認証サーバ１の照合の結果、顧客が認証サーバ１によって認証された場合には自動あるいは手動によって改札の通過を許可する。併せて、入場の場合には発駅を記録し、退場の場合には発駅から着駅までの料金を認証サーバ１のデータベース２に予め登録された決済口座から決済する。発駅の記録並びに着駅までの料金算出等については、認証サーバ１が付随して提供する形態でもよく、また公共交通機関が独自に用意したサーバが提供する形態でも良い。

【００５８】

すなわち、認証サーバ１は認証端末４からの個人認証データの送付であれば（図９ステップＳ６１）、送付されたデータと予め登録してある個人認証データとを照合し（図９ステップＳ６２）、顧客が本人であるかどうかを確認する（図９ステップＳ６３）。

【００５９】

認証サーバ１はこの個人認証において不一致を検出すると、本人でないことを認証端末４に送付し（図９ステップＳ６４）、一致を検出すると、本人であることを認証端末４に送付する（図９ステップＳ６５）。

【００６０】

この一致を検出した時、認証サーバ１は改札の通過許可を認証端末４に通知し（図９ステップＳ６６）、改札からの入場であれば（図９ステップＳ６７）、発駅を記録する（図９ステップＳ６８）。

【００６１】

また、認証サーバ１は改札からの入場でなければ（図９ステップＳ６７）、発駅から着駅までの料金を算出し、データベース２に予め登録してある決済口座からの料金の支払いの処理を実行する（図９ステップＳ６９）。

【００６２】

これによって、定期券や切符の所持携行を忘れたり、あるいは定期券や切符を紛失したためにサービスの提供を受けることができないということがない。この場合、紛失した定期券や切符が第３者に悪用される恐れもない。

【００６３】

また、公共交通機関のサービスの提供を受ける際にクレジット会社のサービスを利用する場合に、従来、一般的であったクレジットカードが不要であるため、クレジットカードの所持携行を忘れたり、あるいはクレジットカードを紛失したためにサービスの提供を受けることができないということがない。この場合も、紛失したクレジットカードが第３者に悪用される恐れもない。

【００６４】

図１０は本発明の第７の実施例による認証サーバの処理動作を示すフローチャートである。この図１０を参照して本発明の第７の実施例による認証サーバの処理動作について説明する。ここで、本発明の第７の実施例による個人認証システムの構成及び動作は図１に示す本発明の第１の実施例による個人認証システム、または図４に示す本発明の第２の実施例による個人認証システム、あるいは図６に示す本発明の第４の実施例による個人認証システムを公衆電話サービスに適用した例であり、その構成及び動作は本発明の第１～第４の実施例による個人認証システムと同様であるので、それらの説明については省略する。

【００６５】

本発明の第７の実施例による個人認証システムでは、認証端末４の機能を公衆電話に付加している。顧客は公衆電話を利用する際に、上記と同様の手順によって個人認証を行う。

【００６６】

公衆電話は認証サーバ１のデータベース２の照合の結果、顧客が認証サーバ１によって認証された場合には回線使用を許可する。併せて、通信開始時刻並びに

接続先を記録し、通信終了時には通信料金を認証サーバ１のデータベース２に予め登録された決済口座から決済する。通信時刻、通信先の記録、並びに通信料金算出等は認証サーバ１が付随して提供する形態でもよく、また公衆電話あるいは独自に用意した公衆電話が接続するサーバが提供する形態でも良い。

【００６７】

すなわち、認証サーバ１は認証端末４からの個人認証データの送付であれば（図１０ステップＳ７１）、送付されたデータと予め登録してある個人認証データとを照合し（図１０ステップＳ７２）、顧客が本人であるかどうかを確認する（図１０ステップＳ７３）。

【００６８】

認証サーバ１はこの個人認証において不一致を検出すると、本人でないことを認証端末４に送付し（図１０ステップＳ７４）、一致を検出すると、本人であることを認証端末４に送付する（図１０ステップＳ７５）。

【００６９】

この一致を検出した時、認証サーバ１は回線使用許可を認証端末４に通知し（図１０ステップＳ７６）、通信終了でなければ（図１０ステップＳ７７）、通信開始時刻並びに接続先を記録し（図１０ステップＳ７８）、通信終了の判定に戻る。

【００７０】

また、認証サーバ１は通信終了であれば（図１０ステップＳ７７）、通信料金を算出し、データベース２に予め登録してある決済口座からの料金の支払いの処理を実行する（図１０ステップＳ７９）。

【００７１】

このように、一般の公衆回線サービスを利用する際に、従来、一般的であった現金やプリペイドカード、及びクレジットカード等による決済によらずに料金を支払うことができるため、これらを所持携行していないために回線が利用できないということがない。また、プリペイドカードやクレジットカードが不要であるので、これらのカード類を偽造して違法に利用されるということもない。

【００７２】

図１１は本発明の第８の実施例による認証サーバの処理動作を示すフローチャートである。この図１１を参照して本発明の第８の実施例による認証サーバの処理動作について説明する。ここで、本発明の第８の実施例による個人認証システムの構成及び動作は図１に示す本発明の第１の実施例による個人認証システム、または図４に示す本発明の第２の実施例による個人認証システム、あるいは図６に示す本発明の第４の実施例による個人認証システムを医療機関サービスに適用した例であり、その構成及び動作は本発明の第１～第４の実施例による個人認証システムと同様であるので、それらの説明については省略する。

【００７３】

本発明の第８の実施例による個人認証システムでは、認証端末４を病院窓口に設置している。顧客は病院窓口での受付けの際に、上記と同様の手順によって個人認証を行う。

【００７４】

認証端末４は認証サーバ１のデータベース２の照合の結果、顧客が認証サーバ１によって認証された場合には自動あるいは手動によってカルテの取出し、並びに受診する医科の予約を行う。顧客は診察や治療を受けた後、再び窓口においてカルテの返却を行うとともに、上記と同様の手順によって個人認証を行う。併せて、医療費を認証サーバ１のデータベース２に予め登録された決済口座から決済する。医療費の計算は認証サーバ１が付随して提供する形態でもよく、また病院が独自に用意したサーバが提供する形態でも良い。

【００７５】

すなわち、認証サーバ１は認証端末４からの個人認証データの送付であれば（図１１ステップＳ８１）、送付されたデータと予め登録してある個人認証データとを照合し（図１１ステップＳ８２）、顧客が本人であるかどうかを確認する（図１１ステップＳ８３）。

【００７６】

認証サーバ１はこの個人認証において不一致を検出すると、本人でないことを認証端末４に送付し（図１１ステップＳ８４）、一致を検出すると、本人であることを認証端末４に送付する（図１１ステップＳ８５）。

【００７７】

この一致を検出した時、認証サーバ１は診療または治療の終了でなければ（図１１ステップＳ８６）、カルテの取出し並びに受信医科の予約を行う（図１１ステップＳ８７）。

【００７８】

また、認証サーバ１は診療または治療の終了であれば（図１１ステップＳ８６）、医療費を算出し、データベース２に予め登録してある決済口座からの医療費の支払いの処理を実行する（図１１ステップＳ８８）。

【００７９】

このように、病院にて受診する際に、本人特定に病院発行の受診カード等が不要であるため、これらを盗用されたり、偽造によって悪用される恐れがない。また医療費の支払いにおいても、クレジットカードが不要であるため、これらを所持携行する必要がない。

【００８０】

図１２は本発明の第９の実施例による認証サーバの処理動作を示すフローチャートである。この図１２を参照して本発明の第９の実施例による認証サーバの処理動作について説明する。ここで、本発明の第９の実施例による個人認証システムの構成及び動作は図１に示す本発明の第１の実施例による個人認証システム、または図４に示す本発明の第２の実施例による個人認証システム、あるいは図６に示す本発明の第４の実施例による個人認証システムを官公庁手続きサービスに適用した例であり、その構成及び動作は本発明の第１～第４の実施例による個人認証システムと同様であるので、それらの説明については省略する。

【００８１】

本発明の第９の実施例による個人認証システムでは、認証端末４を官公庁の各種手続き窓口に設置している。顧客は窓口での本人確認が必要な場合に、上記と同様の手順によって個人認証を行う。

【００８２】

また、資格や免許等の官公庁の各種手続きに際して住民票の写し、戸籍抄本あるいは戸籍謄本等の書類提出が必要な場合には認証サーバ１が付随して提供する

か、あるいは官公庁が独自に用意したサーバが提供するこれら書類を提出する。

【００８３】

すなわち、認証サーバ１は認証端末４からの個人認証データの送付であれば（図１２ステップＳ９１）、送付されたデータと予め登録してある個人認証データとを照合し（図１２ステップＳ９２）、顧客が本人であるかどうかを確認する（図１２ステップＳ９３）。

【００８４】

認証サーバ１はこの個人認証において不一致を検出すると、本人でないことを認証端末４に送付し（図１２ステップＳ９４）、一致を検出すると、本人であることを認証端末４に送付する（図１２ステップＳ９５）。

【００８５】

この一致を検出した時、認証サーバ１は資格や免許等の申請受理を許可し、その申請手数料を算出し、データベース２に予め登録してある決済口座からの申請手数料の支払いの処理を実行する（図１２ステップＳ９６）。

【００８６】

このように、官公庁における各種の資格や免許等の申請を行う際に、住民票の写しや戸籍抄本、あるいは戸籍謄本等を事前に用意する必要がなくなり、窓口において本人証明並びにこれらの書類提出を即時行うことができる。

【００８７】

図１３は本発明の第１０の実施例による認証サーバの処理動作を示すフローチャートである。この図１３を参照して本発明の第１０の実施例による認証サーバの処理動作について説明する。ここで、本発明の第１０の実施例による個人認証システムの構成及び動作は図１に示す本発明の第１の実施例による個人認証システム、または図４に示す本発明の第２の実施例による個人認証システム、あるいは図６に示す本発明の第４の実施例による個人認証システムを施設利用サービスに適用した例であり、その構成及び動作は本発明の第１～第４の実施例による個人認証システムと同様であるので、それらの説明については省略する。

【００８８】

本発明の第１０の実施例による個人認証システムでは、認証端末４を図書館や

スポーツジム等の各種サービス提供施設に設置している。顧客は施設利用の受付けの際に、上記と同様の手順によって個人認証を行う。

【００８９】

併せて、施設利用時間の管理や貸し出し図書等の管理を行い、費用処理が必要な場合には、認証サーバ１のデータベース２に予め登録された決済口座から決済する。施設利用時間の管理や貸し出し図書等の管理は認証サーバ１が付随して提供する形態でもよく、またサービス提供施設が独自に用意したサーバが提供する形態でも良い。

【００９０】

すなわち、認証サーバ１は認証端末４からの個人認証データの送付であれば（図１３ステップＳ１０１）、送付されたデータと予め登録してある個人認証データとを照合し（図１３ステップＳ１０２）、顧客が本人であるかどうかを確認する（図１３ステップＳ１０３）。

【００９１】

認証サーバ１はこの個人認証において不一致を検出すると、本人でないことを認証端末４に送付し（図１３ステップＳ１０４）、一致を検出すると、本人であることを認証端末４に送付する（図１３ステップＳ１０５）。

【００９２】

この一致を検出した時、認証サーバ１は図書館やスポーツジム等の各種サービス提供施設への入場であれば（図１３ステップＳ１０６）、各種サービス提供施設への入場を許可し、入場時刻を記録する（図１３ステップＳ１０７）。

【００９３】

また、認証サーバ１は各種サービス提供施設への入場でなければ（図１３ステップＳ１０６）、有料サービスを利用したかを判定する（図１３ステップＳ１０８）。この場合、顧客が有料サービスを利用する毎に記録しておけばよい。

【００９４】

認証サーバ１は顧客が有料サービスを利用していればサービス料金を算出し、データベース２に予め登録してある決済口座からのサービス料金の支払いの処理を実行する（図１３ステップＳ１０９）。

【００９５】

このように、各種サービス提供施設を利用する際に、各サービス提供施設が個別に発行する利用カードや会員証等を所持携行する必要がなくなり、これら利用カードや会員証等を忘れたり、紛失することによってサービス提供を受けられないということがなくなる。

【００９６】

また、上記の各種サービス提供施設への入退場の管理等は個人や法人の敷地、施設等の入退場が制限されている場合にも適用することができ、その場合には認証端末４を個人や法人の敷地、施設等の入退場が制限されている施設への入退場口に設置すればよい。この場合も、顧客は施設入退場の際に、上記と同様の手順によって個人認証を行う。

【００９７】

併せて、必要であれば各顧客の入退場時刻の管理、入場時間の管理、現時点での入場者把握管理等を行う。これらの管理は認証サーバ１が付随して提供する形態でもよく、また各施設が独自に用意したサーバが提供する形態でも良い。

【００９８】

このように、入退場が制限されている施設の入退場の際にも上記の構成及び動作を適用することで、入場許可証や身分証明書等を提示する必要がなくなるため、これらを忘れたり紛失することによって入退場に支障をきたすことがない。また、これらを紛失あるいは盗難されることによって第３者が違法に入退場する恐れもない。

【００９９】

図１４は本発明の第１１の実施例による認証サーバの処理動作を示すフローチャートである。この図１４を参照して本発明の第１１の実施例による認証サーバの処理動作について説明する。ここで、本発明の第１１の実施例による個人認証システムの構成及び動作は図１に示す本発明の第１の実施例による個人認証システム、または図４に示す本発明の第２の実施例による個人認証システム、あるいは図６に示す本発明の第４の実施例による個人認証システムを書類発行・登録サービスに適用した例であり、その構成及び動作は本発明の第１～第４の実施例に

よる個人認証システムと同様であるので、それらの説明については省略する。

【０１００】

本発明の第１１の実施例による個人認証システムでは、認証端末４を市役所や区役所等の住民票の写し、戸籍抄本あるいは戸籍謄本等の書類発行及び登録等の各種手続き窓口に設置している。これらの各種手続き窓口では本人確認が厳格に行われているとはいえず、書類発行や登録等の各種手続きが不正に行われることがある。そこで、本発明をこれらの処理動作にも適用することで不正な処理を排除することができる。その際、顧客は窓口での本人確認が必要な場合に、上記と同様の手順によって個人認証を行う。

【０１０１】

また、これら住民票の写し、戸籍抄本あるいは戸籍謄本等の書類発行や登録等は認証サーバ１が付随して提供するか、あるいは市役所や区役所等が独自に用意したサーバが提供するようにしてもよい。

【０１０２】

すなわち、認証サーバ１は認証端末４からの個人認証データの送付であれば（図１４ステップＳ１１１）、送付されたデータと予め登録してある個人認証データとを照合し（図１４ステップＳ１１２）、顧客が本人であるかどうかを確認する（図１４ステップＳ１１３）。

【０１０３】

認証サーバ１はこの個人認証において不一致を検出すると、本人でないことを認証端末４に送付し（図１４ステップＳ１１４）、一致を検出すると、本人であることを認証端末４に送付する（図１４ステップＳ１１５）。

【０１０４】

この一致を検出した時、認証サーバ１は転居登録や印鑑登録等の各種登録の要求であれば（図１４ステップＳ１１６）、転居登録や印鑑登録等の各種登録の要求の処理を実行する（図１４ステップＳ１１７）。

【０１０５】

また、認証サーバ１は転居登録や印鑑登録等の各種登録の要求でなければ（図１４ステップＳ１１６）、住民票の写し、戸籍抄本あるいは戸籍謄本等の書類の

発行と判断してそれらの書類を発行し、その手数料を算出し、データベース２に予め登録してある決済口座からの手数料の支払いの処理を実行する（図１４ステップＳ１１８）。

【０１０６】

このように、住民票の写し、戸籍抄本あるいは戸籍謄本等の書類の発行、転居登録や印鑑登録等の各種登録が不正に行われるのを未然に防止することができ、それらの手続を行う際に、個人を認証するための運転免許証等の証明書類や印鑑登録カード等を所持携行する必要がなくなり、これら証明書類やカード類等を忘れたり、紛失することによってサービス提供を受けられないということがなくなる。

【０１０７】

【発明の効果】

以上説明したように本発明によれば、顧客が本人であることを証明するための個人認証を行う認証サーバと個人認証を行うための認証情報を入力する認証端末とを通信回線を介して相互に接続する個人認証システムにおいて、予め登録される個人認証を行うための個人認証データと費用処理するための決済口座の情報と各種サービスを受けるために必要なデータとを少なくとも蓄積するデータベースを配置し、認証サーバで、認証端末から通信回線を介して入力される認証情報をデータベースに蓄積された個人認証データと照会して本人確認を行い、本人確認で認証された時に認証端末からの要求に基づいてデータベースに登録された決済口座の情報を基に費用処理し、本人確認で認証された時に認証端末からの要求に基づいてデータベースに予め登録された個人データの提供と登録と管理とを行うとともに、それらの照会履歴と個人データ利用履歴と費用処理履歴とを定期的に通知することによって、カード類の所持携行を忘れたりあるいはカード類を紛失した場合でもサービスの提供を受けることができ、カード類の第３者による悪用を防止することができるとともに、個人情報の流出を防止することができるという効果がある。

【図面の簡単な説明】

【図１】

本発明の第１の実施例による個人認証システムの構成を示すブロック図である。

【図２】

図１の認証サーバの処理動作を示すフローチャートである。

【図３】

図１の認証サーバの処理動作を示すフローチャートである。

【図４】

本発明の第２の実施例による個人認証システムの構成を示すブロック図である。

【図５】

本発明の第３の実施例による認証サーバの処理動作を示すフローチャートである。

【図６】

本発明の第４の実施例による個人認証システムの構成を示すブロック図である。

【図７】

図６の認証サーバの処理動作を示すフローチャートである。

【図８】

本発明の第５の実施例による認証サーバの処理動作を示すフローチャートである。

【図９】

本発明の第６の実施例による認証サーバの処理動作を示すフローチャートである。

【図１０】

本発明の第７の実施例による認証サーバの処理動作を示すフローチャートである。

【図１１】

本発明の第８の実施例による認証サーバの処理動作を示すフローチャートである。

【図１２】

本発明の第９の実施例による認証サーバの処理動作を示すフローチャートである。

【図１３】

本発明の第１０の実施例による認証サーバの処理動作を示すフローチャートである。

【図１４】

本発明の第１１の実施例による認証サーバの処理動作を示すフローチャートである。

【符号の説明】

１　認証サーバ

２　データベース

３　顧客端末

４　認証端末

５　個人認証データ入力機構

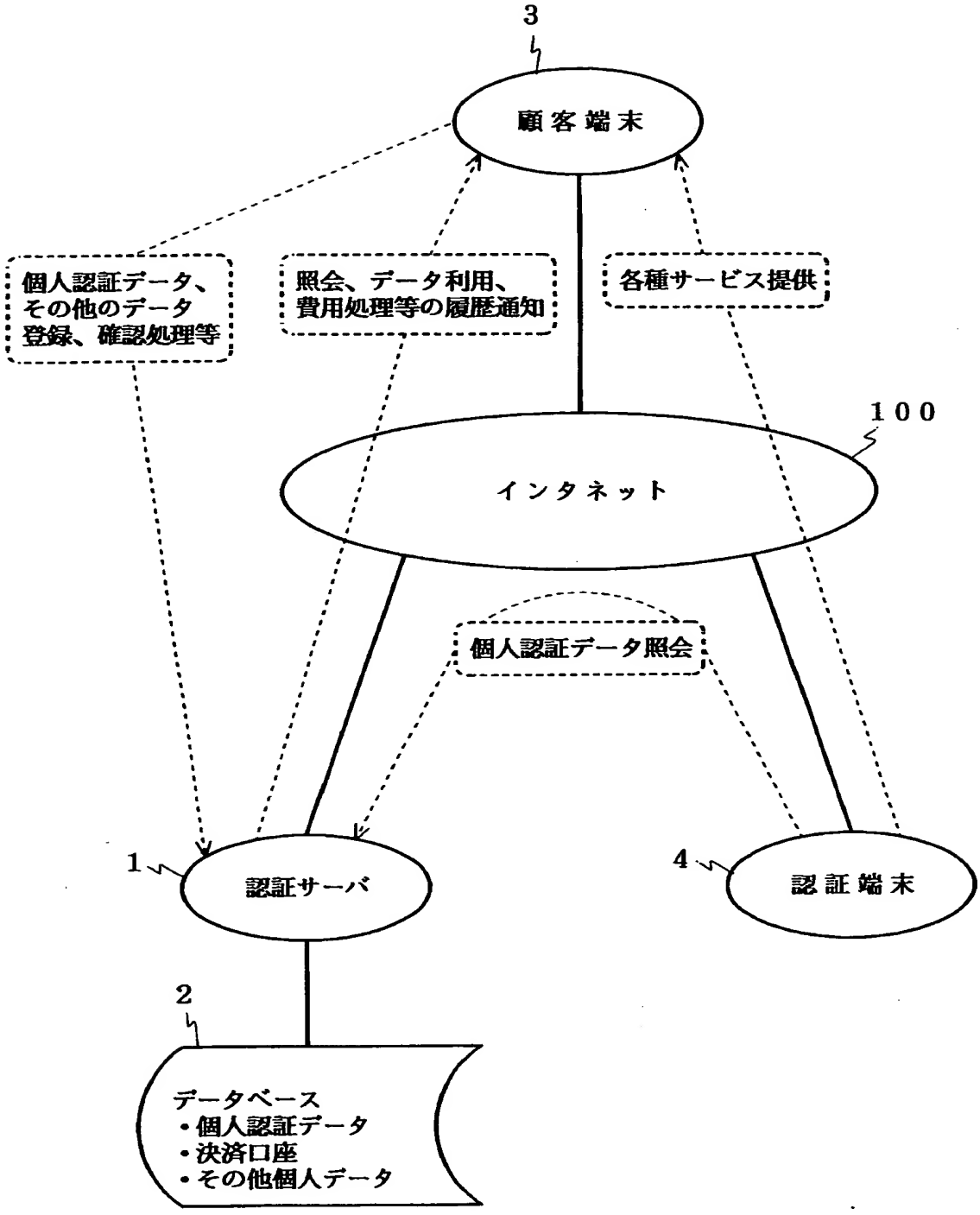
６　掲示用サーバ

７　本人確認機構

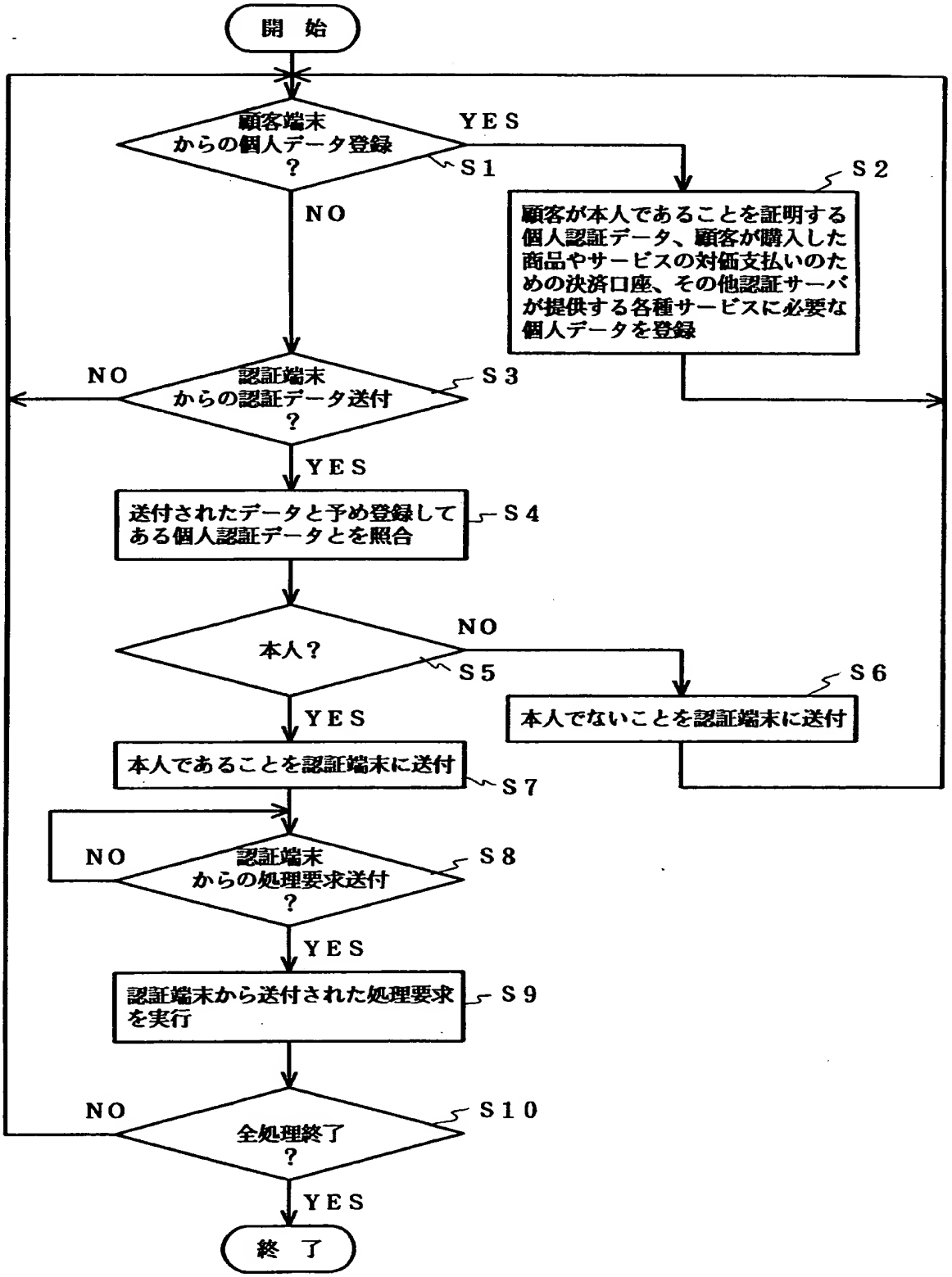
１００　通信回線

【書類名】　　図面

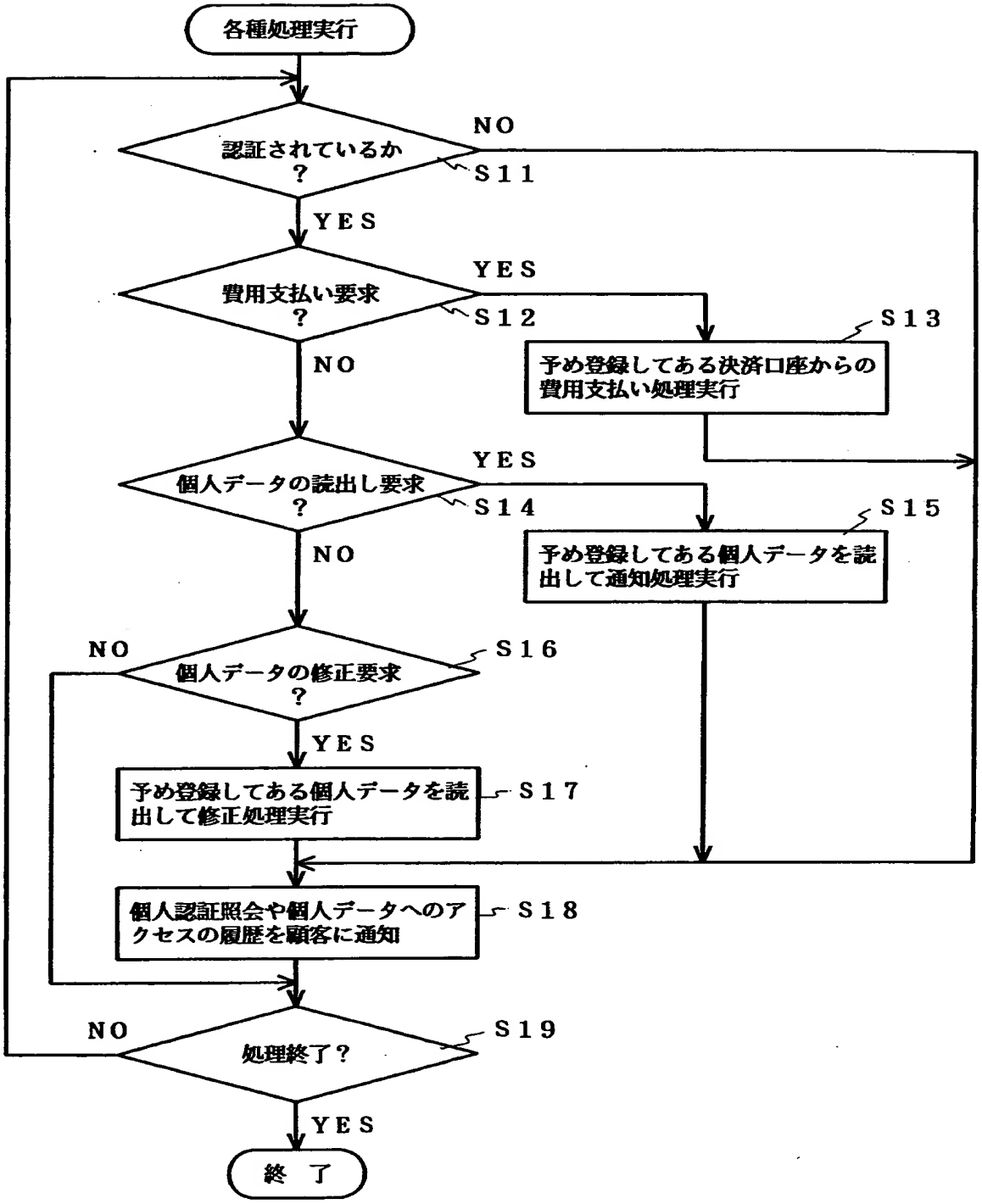
【図１】


3
顧客端末
個人認証データ、
その他のデータ
登録、確認処理等
照会、データ利用、
費用処理等の履歴通知
各種サービス提供
100
インタネット
個人認証データ照会
1
認証サーバ
4
認証端末
2
データベース
・個人認証データ
・決済口座
・その他個人データ

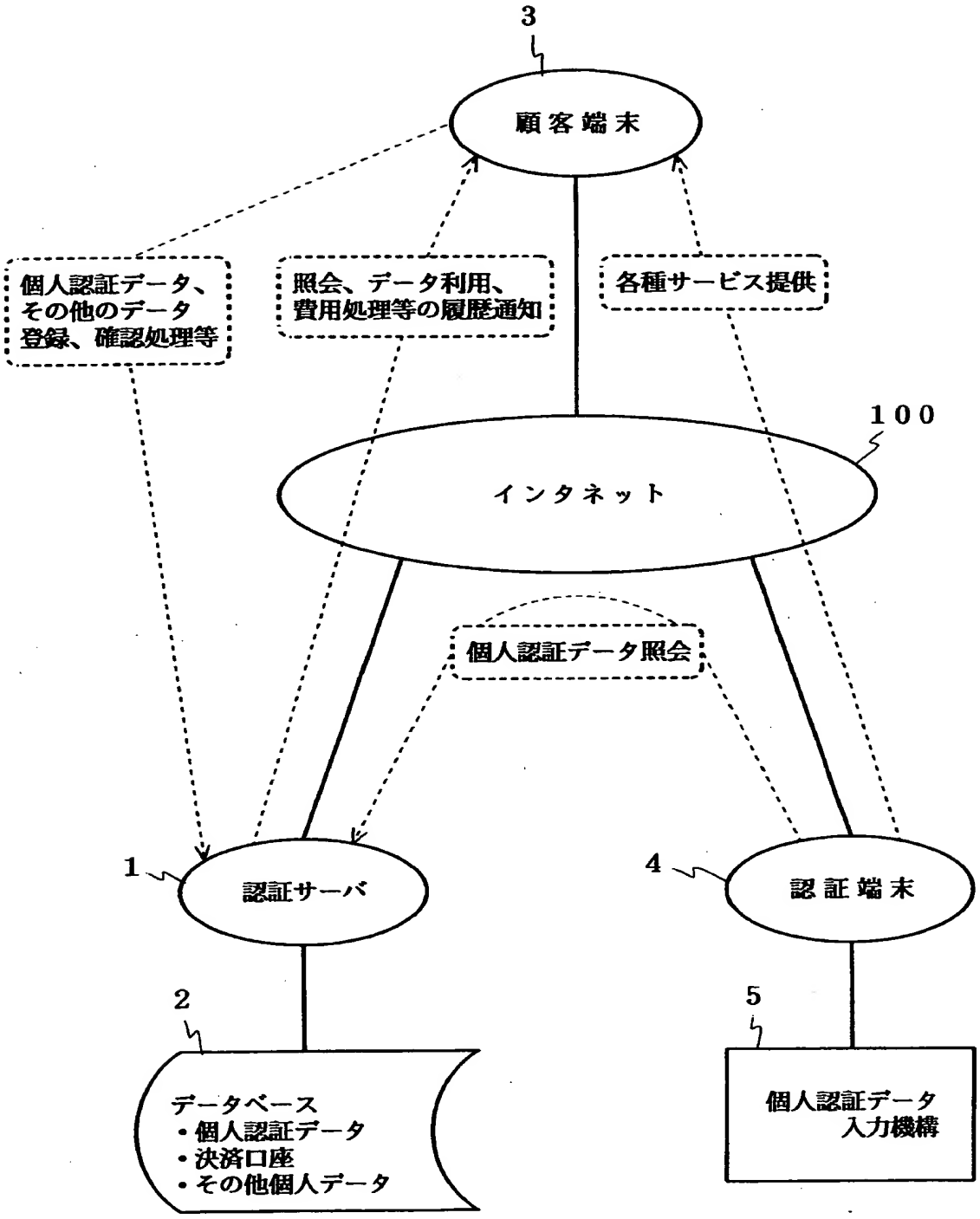
【図２】


開　始
顧客端末からの個人データ登録？
YES
S1
S2
顧客が本人であることを証明する個人認証データ、顧客が購入した商品やサービスの対価支払いのための決済口座、その他認証サーバが提供する各種サービスに必要な個人データを登録
NO
認証端末からの認証データ送付？
NO
S3
YES
送付されたデータと予め登録してある個人認証データとを照合
S4
本人？
NO
S5
S6
本人でないことを認証端末に送付
YES
本人であることを認証端末に送付
S7
認証端末からの処理要求送付？
NO
S8
YES
認証端末から送付された処理要求を実行
S9
全処理終了？
NO
S10
YES
終　了

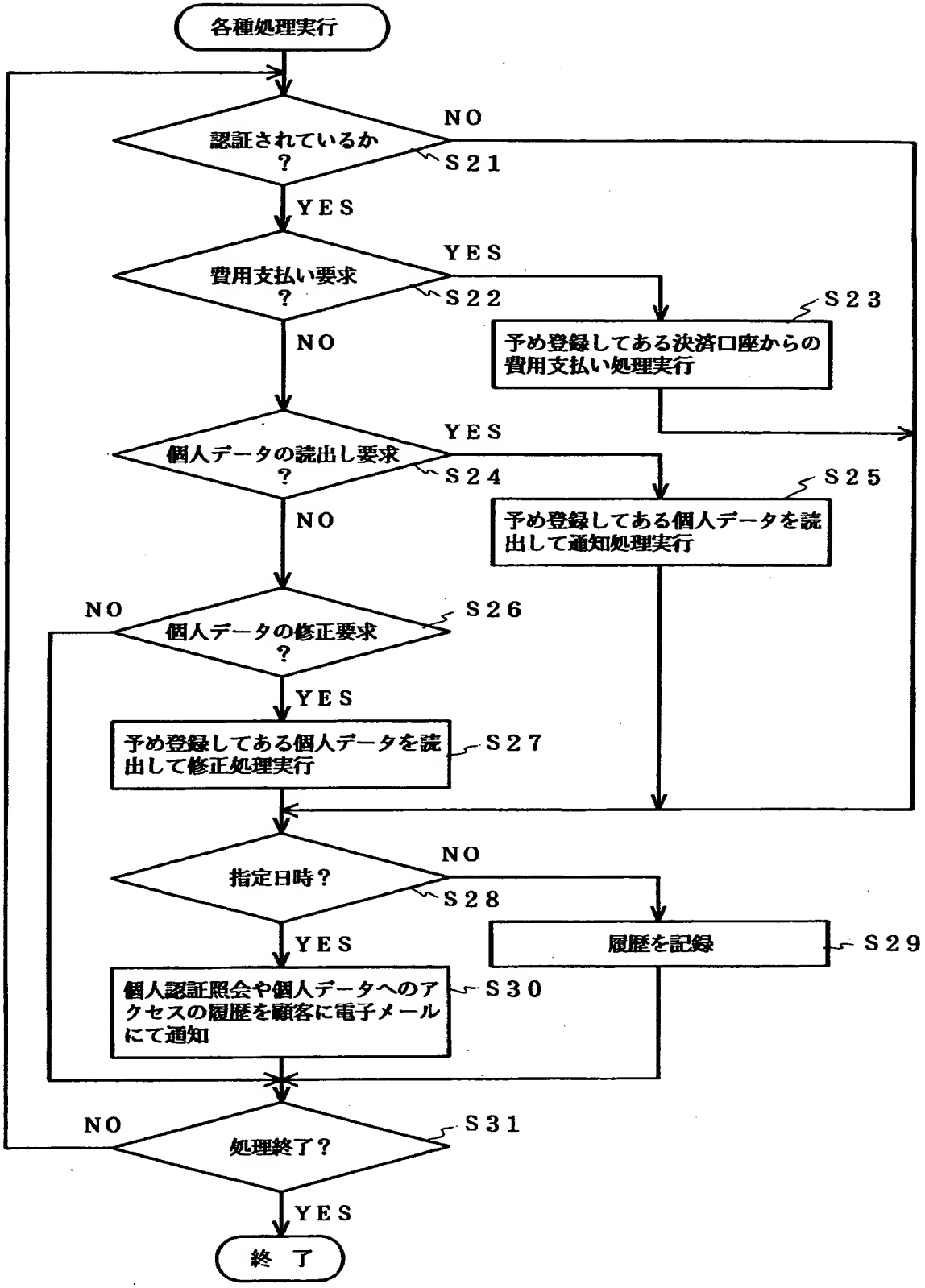
【図３】


各種処理実行
認証されているか？
NO
S１１
YES
費用支払い要求？
YES
S１２
S１３
予め登録してある決済口座からの費用支払い処理実行
NO
個人データの読出し要求？
YES
S１４
S１５
予め登録してある個人データを読出して通知処理実行
NO
個人データの修正要求？
NO
S１６
YES
予め登録してある個人データを読出して修正処理実行
S１７
個人認証照会や個人データへのアクセスの履歴を顧客に通知
S１８
処理終了？
NO
S１９
YES
終　了

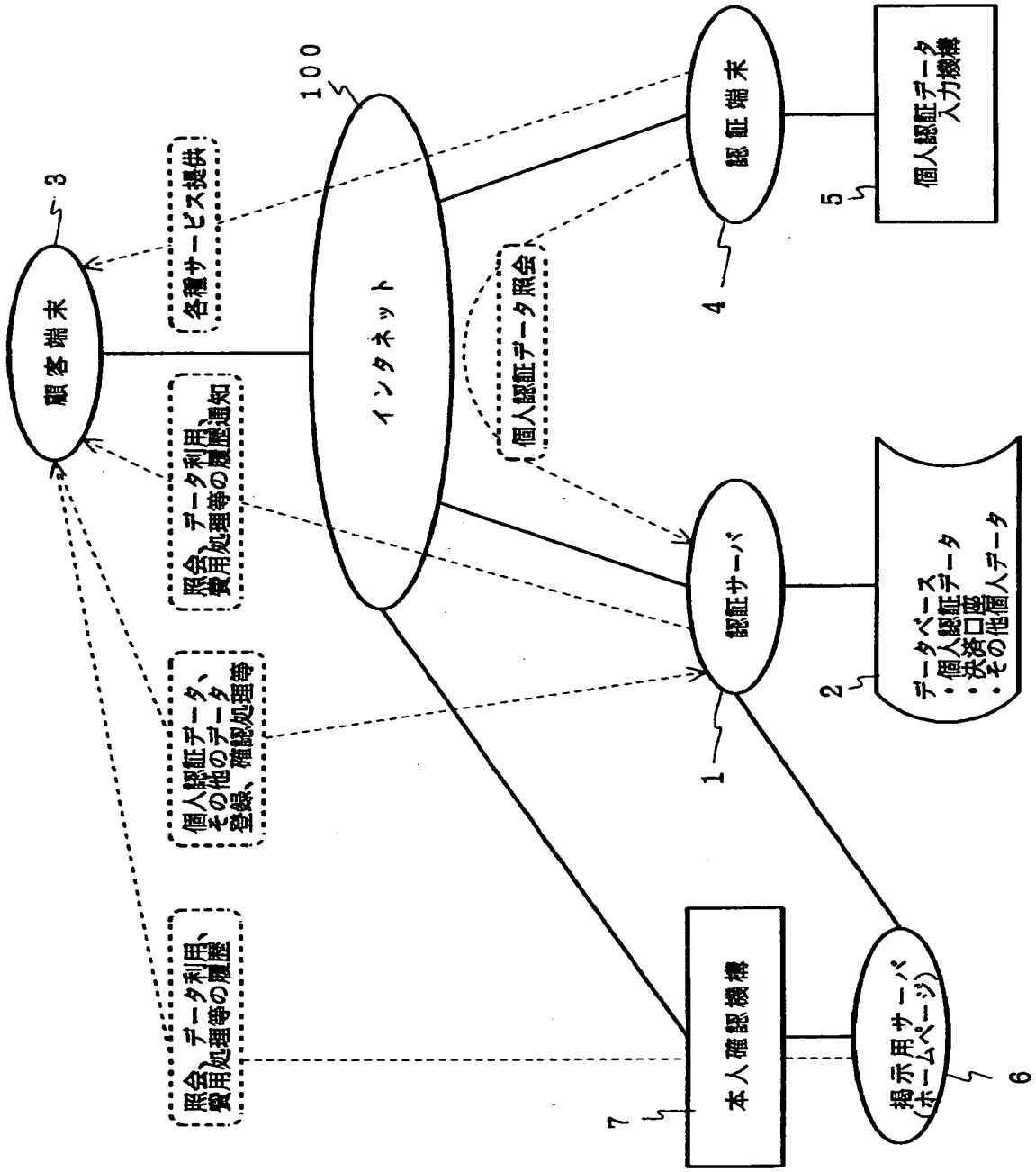
【図４】


3
顧客端末
個人認証データ、
その他のデータ
登録、確認処理等
照会、データ利用、
費用処理等の履歴通知
各種サービス提供
100
インタネット
個人認証データ照会
1
認証サーバ
4
認証端末
2
データベース
・個人認証データ
・決済口座
・その他個人データ
5
個人認証データ
入力機構

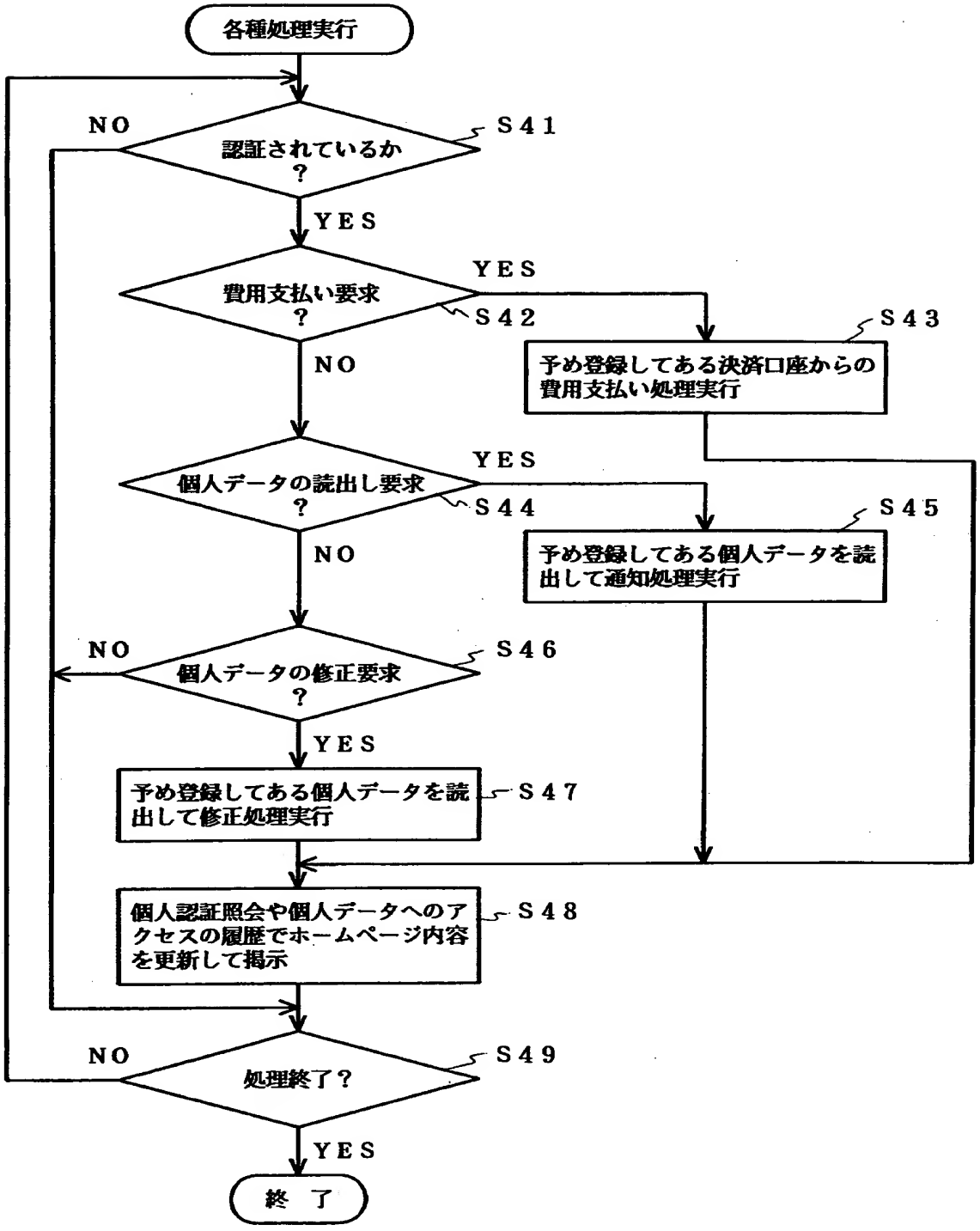
【図５】


各種処理実行
認証されているか？
NO
S２１
YES
費用支払い要求？
YES
S２２
S２３
予め登録してある決済口座からの費用支払い処理実行
NO
個人データの読出し要求？
YES
S２４
S２５
予め登録してある個人データを読出して通知処理実行
NO
個人データの修正要求？
NO
S２６
YES
予め登録してある個人データを読出して修正処理実行
S２７
指定日時？
NO
S２８
YES
履歴を記録
S２９
個人認証照会や個人データへのアクセスの履歴を顧客に電子メールにて通知
S３０
処理終了？
NO
S３１
YES
終　了

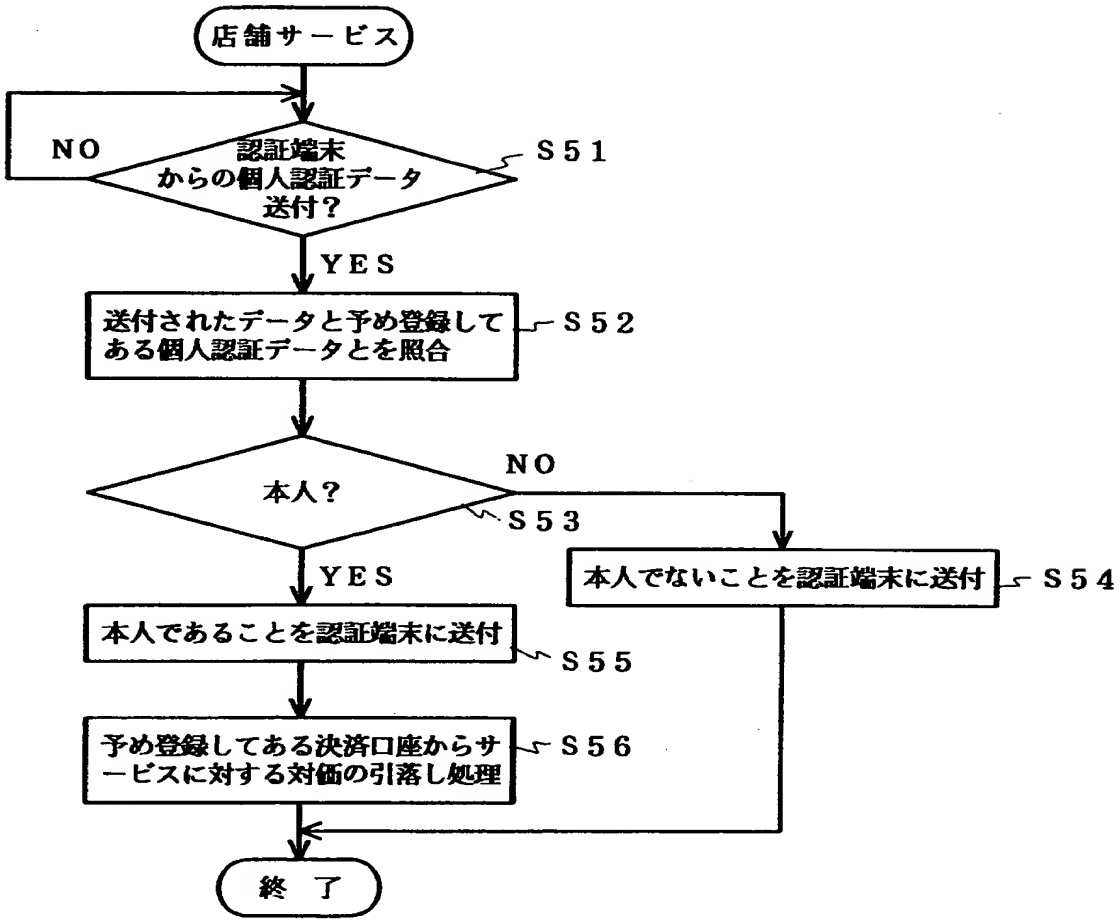
【図６】


顧客端末
3
インターネット
100
各種サービス提供
照会、データ利用、費用処理等の履歴通知
個人認証データ、その他のデータ、登録、確認処理等
照会、データ利用、費用処理等の履歴
個人認証データ照会
認証端末
4
個人認証データ入力機構
5
認証サーバ
1
データベース
・個人認証データ
・決済口座
・その他個人データ
2
本人確認機構
7
掲示用サーバ（ホームページ）
6

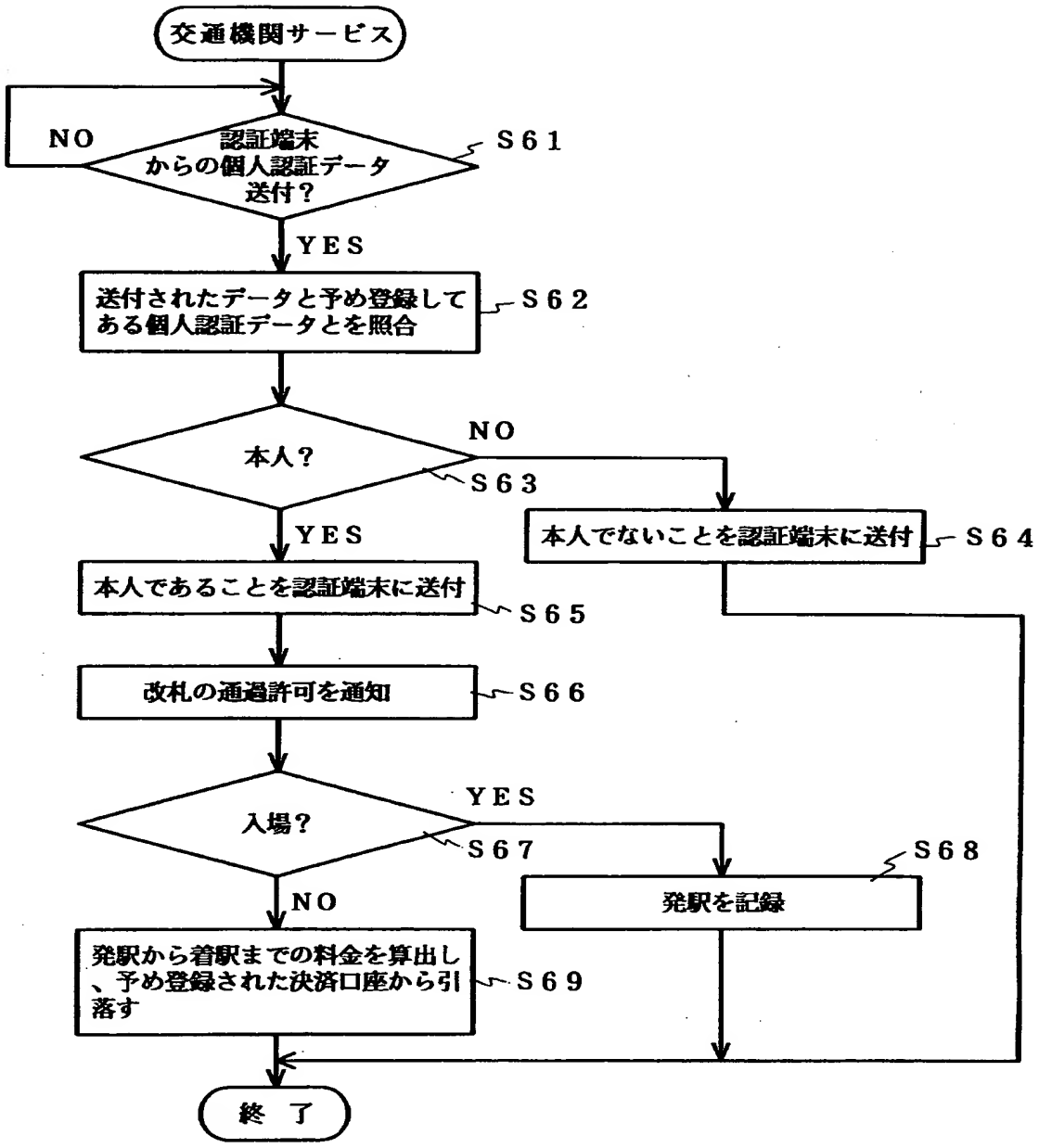
【図７】


各種処理実行
認証されているか？
S41
NO
YES
費用支払い要求？
S42
YES
NO
S43
予め登録してある決済口座からの費用支払い処理実行
個人データの読出し要求？
S44
YES
NO
S45
予め登録してある個人データを読出して通知処理実行
個人データの修正要求？
S46
NO
YES
予め登録してある個人データを読出して修正処理実行
S47
個人認証照会や個人データへのアクセスの履歴でホームページ内容を更新して掲示
S48
処理終了？
S49
NO
YES
終　了

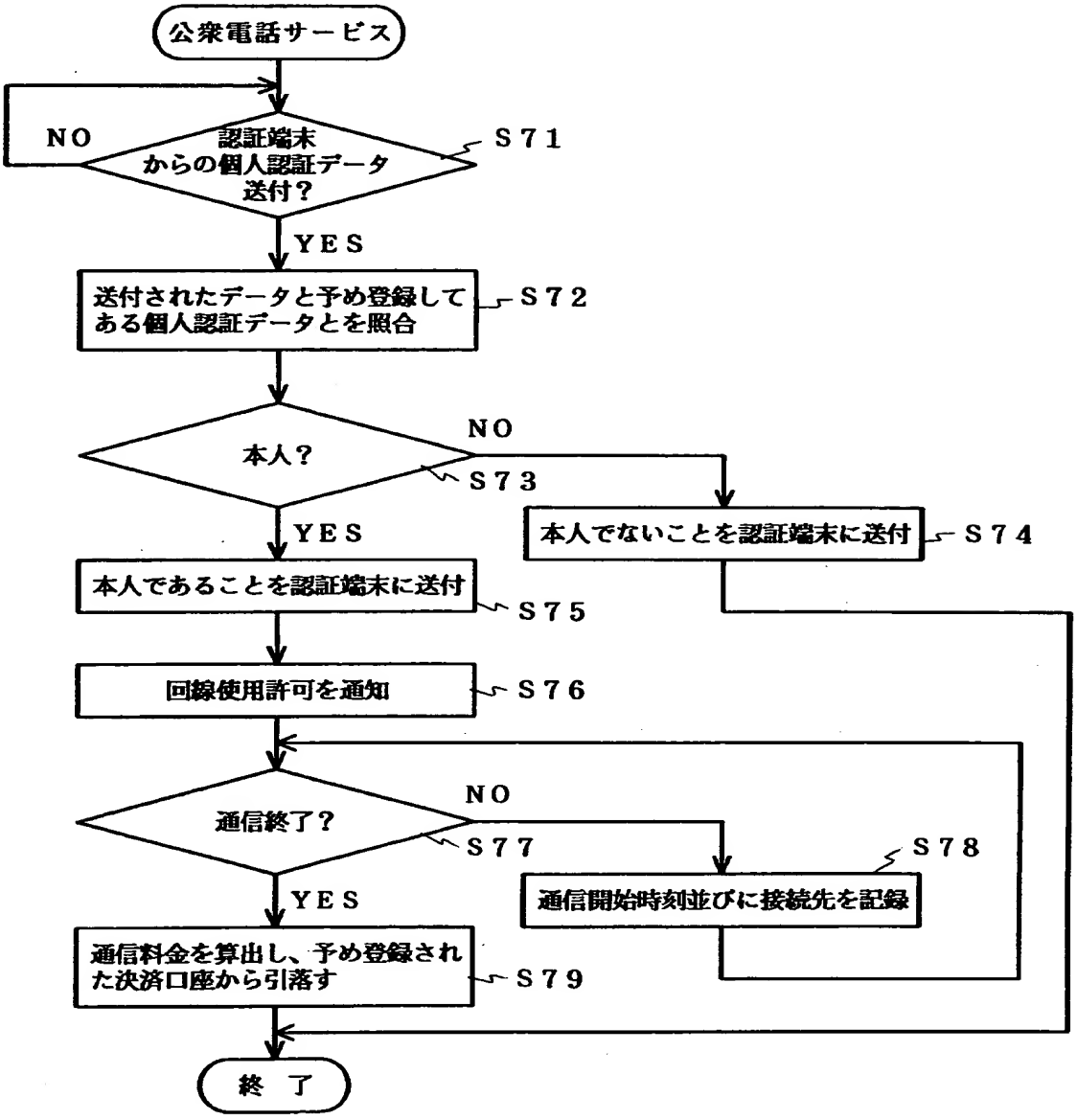
【図８】


店舗サービス
NO
認証端末からの個人認証データ送付？
S51
YES
送付されたデータと予め登録してある個人認証データとを照合
S52
本人？
NO
S53
YES
本人でないことを認証端末に送付
S54
本人であることを認証端末に送付
S55
予め登録してある決済口座からサービスに対する対価の引落し処理
S56
終了

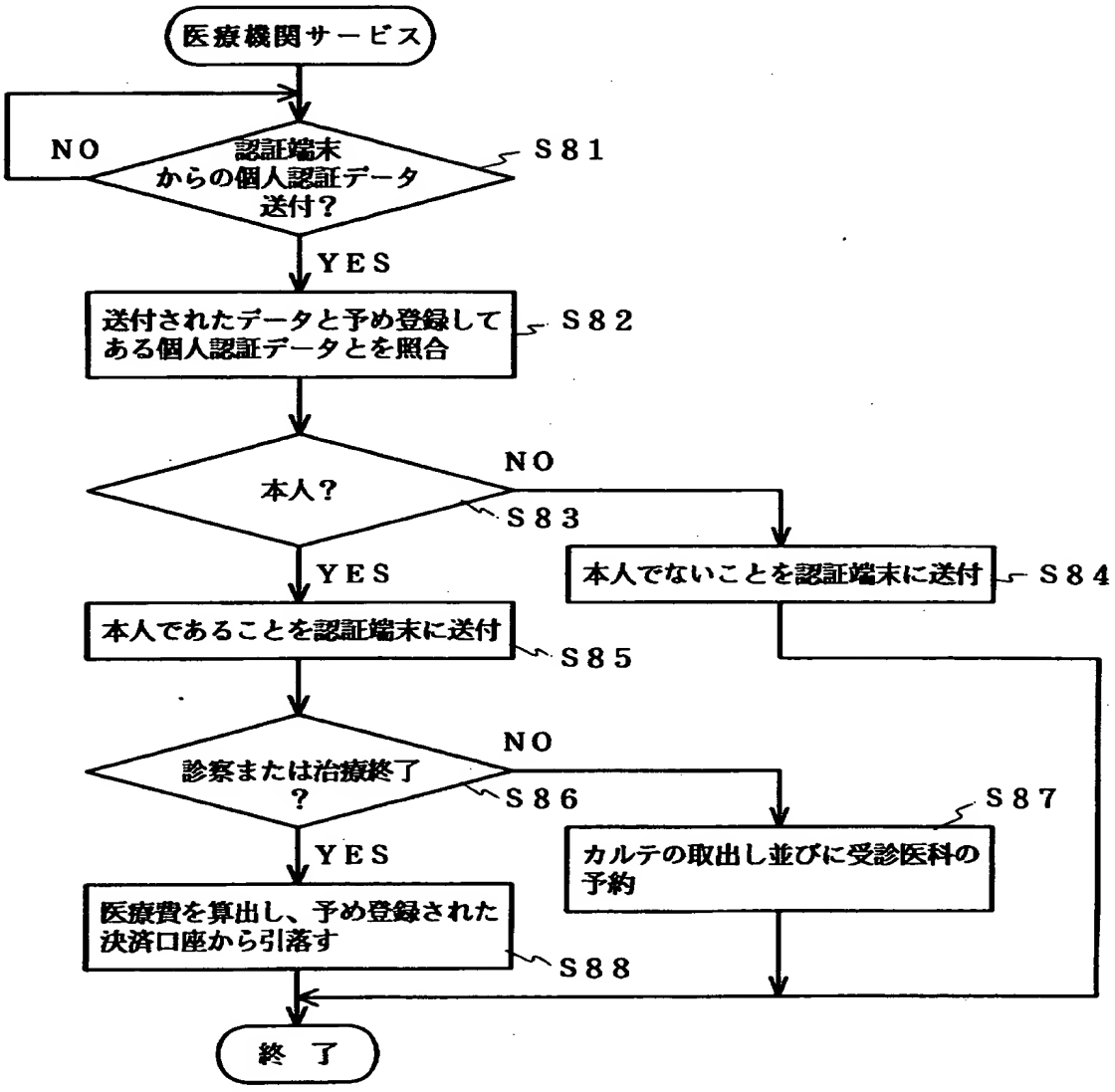
【図９】


交通機関サービス
認証端末からの個人認証データ送付？
NO
S６１
YES
送付されたデータと予め登録してある個人認証データとを照合
S６２
本人？
NO
S６３
YES
本人でないことを認証端末に送付
S６４
本人であることを認証端末に送付
S６５
改札の通過許可を通知
S６６
入場？
YES
S６７
S６８
発駅を記録
NO
発駅から着駅までの料金を算出し、予め登録された決済口座から引落す
S６９
終　了

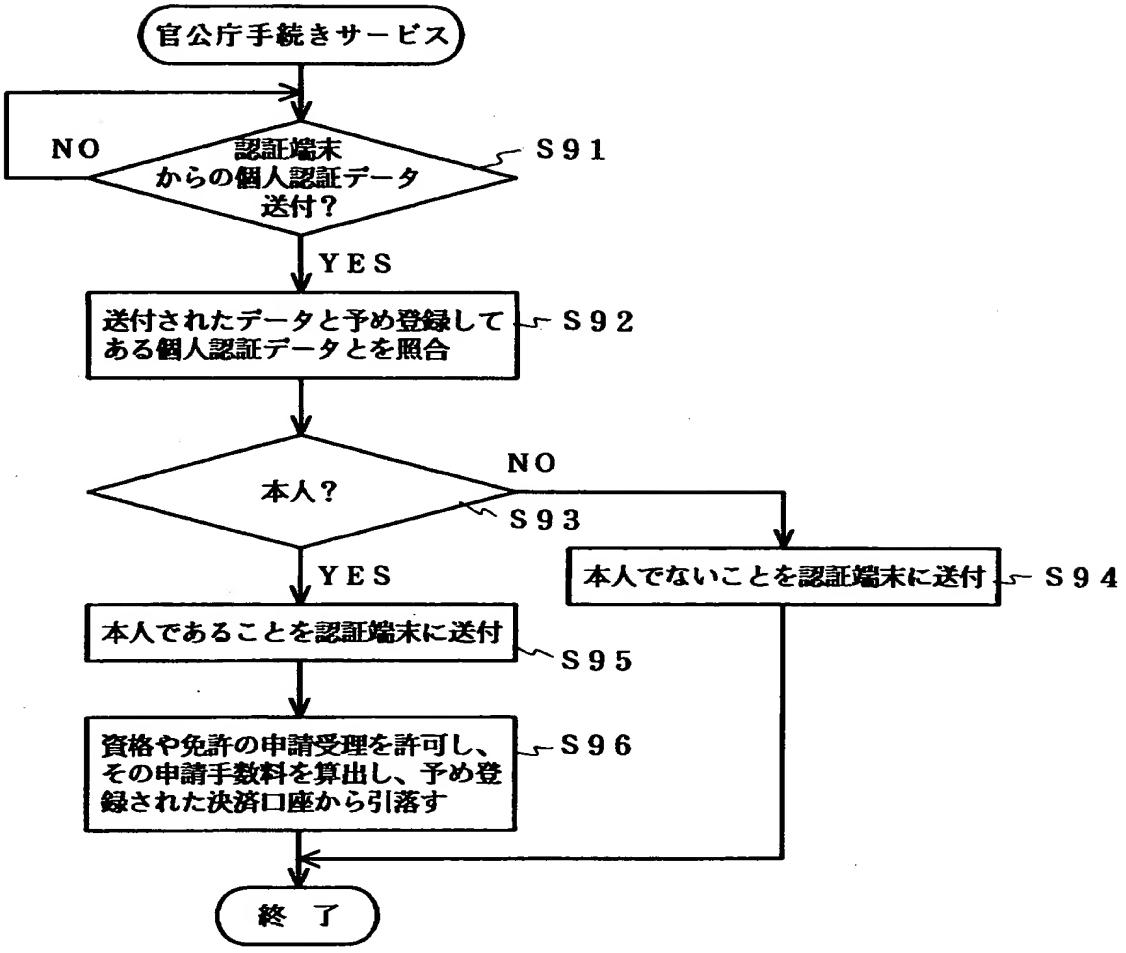
【図１０】


公衆電話サービス
認証端末からの個人認証データ送付？
NO
S71
YES
送付されたデータと予め登録してある個人認証データとを照合
S72
本人？
NO
S73
YES
本人でないことを認証端末に送付
S74
本人であることを認証端末に送付
S75
回線使用許可を通知
S76
通信終了？
NO
S77
S78
通信開始時刻並びに接続先を記録
YES
通信料金を算出し、予め登録された決済口座から引落す
S79
終了

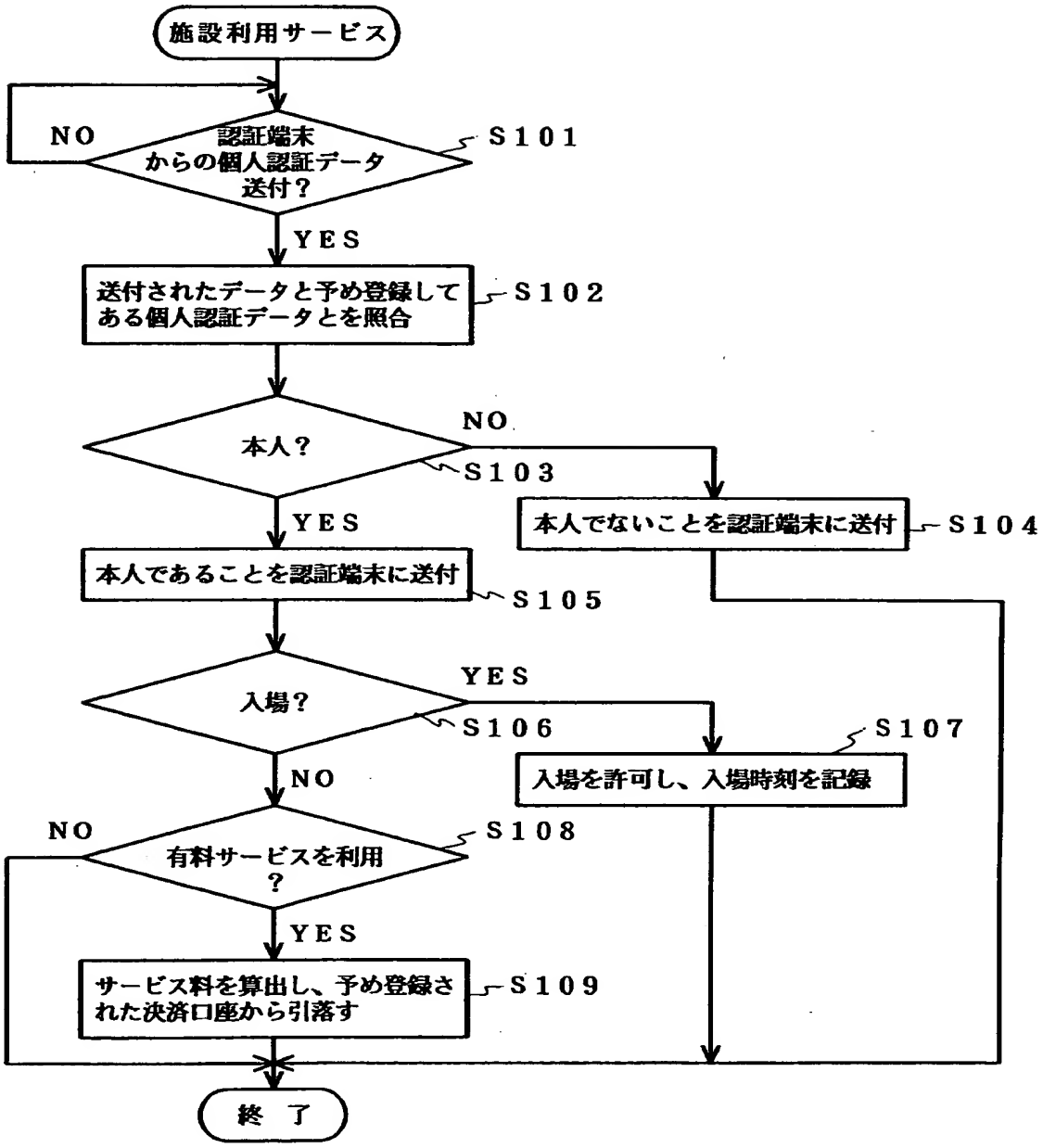
【図１１】


医療機関サービス
NO
認証端末からの個人認証データ送付？
S81
YES
送付されたデータと予め登録してある個人認証データとを照合
S82
本人？
NO
S83
YES
本人でないことを認証端末に送付
S84
本人であることを認証端末に送付
S85
診察または治療終了？
NO
S86
S87
YES
カルテの取出し並びに受診医科の予約
医療費を算出し、予め登録された決済口座から引落す
S88
終 了

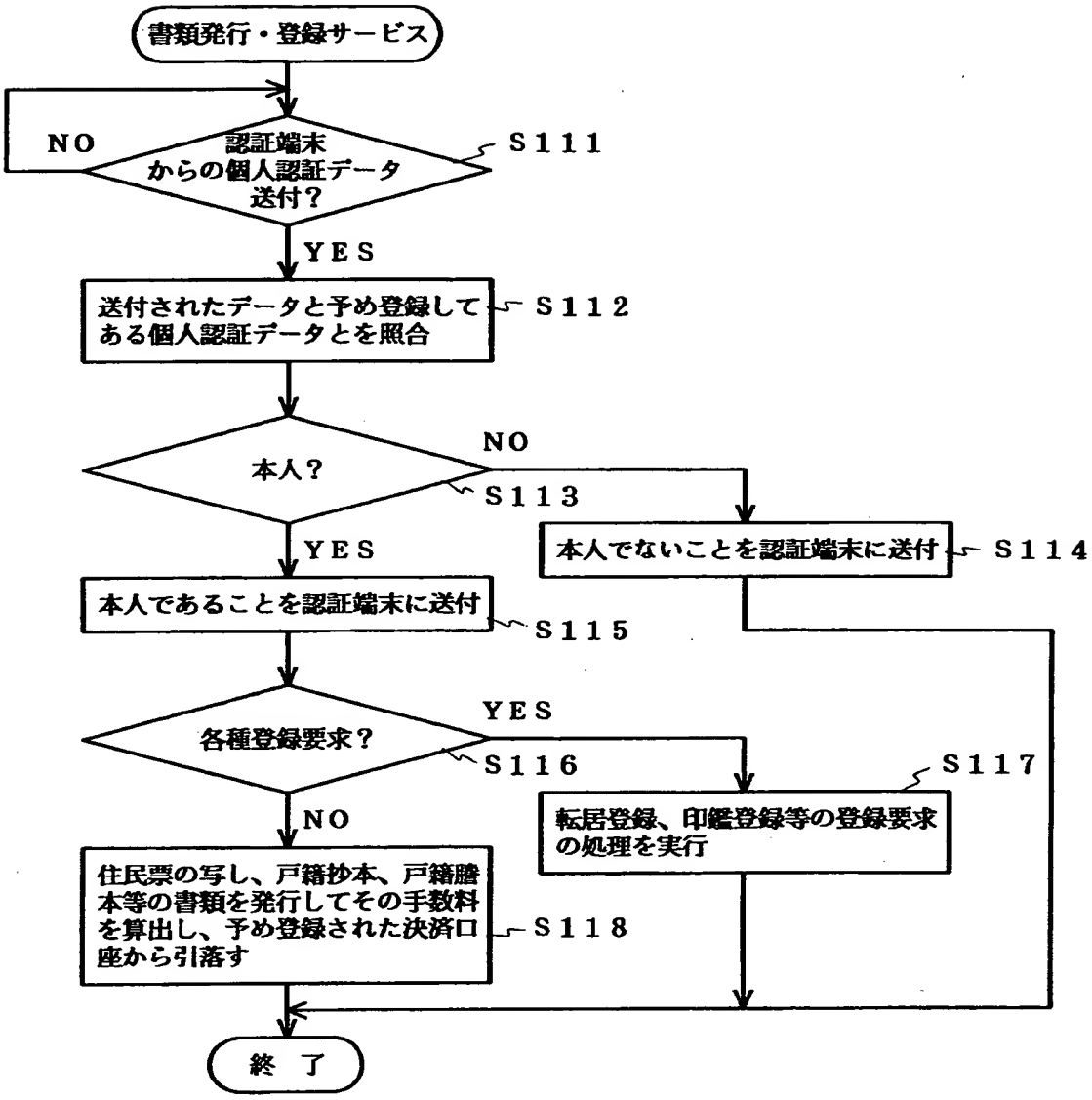
【図１２】


官公庁手続きサービス
NO
認証端末からの個人認証データ送付？
S91
YES
送付されたデータと予め登録してある個人認証データとを照合
S92
本人？
NO
S93
YES
本人でないことを認証端末に送付
S94
本人であることを認証端末に送付
S95
資格や免許の申請受理を許可し、その申請手数料を算出し、予め登録された決済口座から引落す
S96
終了

【図１３】


施設利用サービス
NO
認証端末からの個人認証データ送付？
S１０１
YES
送付されたデータと予め登録してある個人認証データとを照合
S１０２
本人？
NO
S１０３
YES
本人でないことを認証端末に送付
S１０４
本人であることを認証端末に送付
S１０５
入場？
YES
S１０６
S１０７
入場を許可し、入場時刻を記録
NO
NO
有料サービスを利用？
S１０８
YES
サービス料を算出し、予め登録された決済口座から引落す
S１０９
終　了

【図１４】


書類発行・登録サービス
認証端末からの個人認証データ送付？
NO
S111
YES
送付されたデータと予め登録してある個人認証データとを照合
S112
本人？
NO
S113
YES
本人でないことを認証端末に送付
S114
本人であることを認証端末に送付
S115
各種登録要求？
YES
S116
S117
転居登録、印鑑登録等の登録要求の処理を実行
NO
住民票の写し、戸籍抄本、戸籍謄本等の書類を発行してその手数料を算出し、予め登録された決済口座から引落す
S118
終　了

【書類名】　　要約書

【要約】

【課題】　カード類の所持携行を忘れたりあるいはカード類を紛失した場合でもサービスの提供を受けられ、カード類の第３者による悪用を防止可能とともに、個人情報の流出を防止可能な個人認証システムを提供する。

【解決手段】　認証端末４を用いて顧客が本人であることを証明するデータが送付されてくると、認証サーバ１はその送付されてきたデータと予めデータベース２に登録してある個人認証データとを照合して本人であるかを確認し、その結果を認証端末４に送付する。認証後に、認証端末４からデータベース２に予め登録してある決済口座からの費用支払いや個人データの読出し及び修正等が要求されてくると、認証サーバ１は送付された要求に基づいて処理を行う。認証サーバ１はこれらの個人認証照会や個人データへのアクセスの履歴を顧客に通知する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００１９０５４１〕

１．変更年月日　　１９９０年　８月１０日
［変更理由］　新規登録
住　所　　新潟県柏崎市大字安田７５４６番地
氏　名　　新潟日本電気株式会社